TEORIA CALITATIVĂ A ECUAȚIILOR ALGEBRICE

C. NĂSTĂSESCU * C. NIȚA



CUPRINS

INTRODUCERE

În lucrare este tratată în principal problema rezolvării prin radicali a ecuațiilor algebrice cu coeficienți complecși.

Se numește ecuație algebrică de gradul n o ecuație de forma

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0,$$

unde $a_1, a_2, \ldots, a_n$ sînt numere complexe.

Rezolvarea ecuațiilor algebrice prin radicali i-a preocupat pe matematicieni de peste 2 000 de ani. Este suficient să reamintim că formulele de rezolvare a ecuațiilor de gradul al doilea erau cunoscute încă de la babilonieni, iar pentru ecuațiile algebrice de gradul al treilea și al patrulea, formulele de rezolvare sînt cunoscute din perioada Renașterii italiene. Rezolvarea ecuațiilor algebrice de grad mai mare sau egal cu cinci a stat în continuare în atenția matematicienilor (este suficient să reamintim aici pe Euler, Descartes, Lagrange) dar abia la începutul secolului al XIX-lea a fost demostrată de către Abel și Ruffini imposibilitatea găsirii unor formule de rezolvare pentru ecuațiile de grad mai mare sau egal cu cinci. Problema rezolvării ecuațiilor algebrice a fost complet tranșată odată cu apariția teoriei lui Galois cînd au fost date criterii de rezolvabilitate a ecuațiilor prin radicali.

Lucrarea are opt capitole. Primele trei capitole sînt pregătitoare, prezentînd noțiunile de bază necesare în celelalte capitole. În capitolul IV sînt prezentate metode elementare de găsire a formulelor de rezolvare pentru ecuațiile de grad mai mic sau egal cu patru. Capitolul V prezintă metode numerice de determinare aproximativă a rădăcinilor reale ale unei ecuații

algebrice cu coeficienţi reali. Ultimele trei capitole prezintă teoria lui Galois cu aplicaţii la rezolvarea ecuaţiilor algebrice, precum şi la problema construcţiilor geometrice cu rigla şi compasul (problemă de asemenea veche, datînd din antichitate).

Această lucrare prezintă toate noţiunile necesare înţelegerii ei, începînd cu numere complexe, elemente de teoria grupurilor etc. şi sfîrşind cu elemente de teoria corpurilor, teoria lui Galois etc., fiind accesibilă unei mase largi de cititori.

Pe parcursul lucrării am notat cu $\mathbb{N}$ mulţimea numerelor naturale $\{0, 1, 2, \ldots\}$, cu $\mathbb{Z}$ mulţimea numerelor întregi, cu $\mathbb{Q}$ mulţimea numerelor raţionale iar cu $\mathbb{R}$ mulţimea numerelor reale.

AUTORII

I

NUMERE COMPLEXE

§ 1. Mulțimea numerelor complexe

În matematică, noțiunea de număr a avut o evoluție progresivă. La început, se face cunoștință cu mulțimea $\mathbb{N}$ a numerelor naturale. Dar imposibilitatea de a face unele operații simple, rezultate din operațiile fundamentale, ne conduce la lărgirea repetată a acestei mulțimi. Mai întîi, se introduc numerele întregi negative, obținîndu-se astfel o mulțime mai largă și anume mulțimea $\mathbb{Z}$ a numerelor întregi formată din numere întregi pozitive (naturale) nenule, negative și zero. Apoi, această mulțime se lărgește la mulțimea $\mathbb{Q}$ a numerelor raționale, care este mai bogată. Se extinde încă noțiunea de număr, completînd mulțimea numerelor raționale cu numere iraționale, obținîndu-se astfel mulțimea $\mathbb{R}$ a numerelor reale. Fundamentarea matematică riguroasă a teoriei acestor mulțimi nu constituie obiectul acestei cărți, cunoștințele căpătate în școala medie despre acestea fiind suficiente pentru a aborda problematica lucrării de față.

Să considerăm problema rezolvării unei ecuații de gradul al doilea cu coeficienți reali. Mulțimea numerelor reale nu se dovedește suficient de largă pentru a putea găsi rădăcini ale oricărei ecuații de acest tip. Cea mai simplă ecuație de gradul al doilea care nu are rădăcini reale este

$$x^2 + 1 = 0.$$

Se pune problema lărgirii conceptului de număr real, introducînd o mulţime de numere mai bogată, în aşa fel, ca această ecuaţie să aibă soluţii. În această nouă mulţime, ridicarea la o putere oarecare are întotdeauna sens. Noua mulţime care se obţine va fi mulţimea $\mathbb{C}$ a numerelor complexe, de care ne vom ocupa în continuare. Mai întîi prezentăm construcţia sa, plecînd de la mulţimea $\mathbb{R}$ a numerelor reale.

Fie produsul cartezian

$$\mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}.$$

Convenim să notăm cu litere greceşti elementele mulţimii $\mathbb{R} \times \mathbb{R}$. Pe această mulţime se definesc două operaţii algebrice şi anume *adunarea* şi *înmulţirea*.

Fie $\alpha = (a, b)$ şi $\alpha' = (a', b')$ care aparţin lui $\mathbb{R} \times \mathbb{R}$. Dacă $(a, b) + (a', b') = (a + a', b + b')$, atunci elementul $(a + a', b + b')$ se numeşte *suma* dintre α şi α' iar operaţia prin care oricăror α şi α' din $\mathbb{R} \times \mathbb{R}$ li se asociază suma lor se numeşte *adunare*.

De asemenea dacă $(a, b)(a', b') = (aa' - bb', ab' + a'b)$, elementul $(aa' - bb', ab' + a'b)$ se numeşte *produsul* dintre α şi α' iar operaţia prin care oricăror α şi α' din $\mathbb{R} \times \mathbb{R}$ li se asociază produsul lor se numeşte *înmulţire*.

Definiţia 1.1. Fiecare element al mulţimii $\mathbb{R} \times \mathbb{R}$ pe care sînt definite cele două operaţii se numeşte *număr complex*. Se notează cu $\mathbb{C}$ mulţimea numerelor complexe.

Arătăm acum că numerele reale sînt un caz particular de numere complexe. Fie pentru aceasta mulţimea

$$\overline{\mathbb{R}} = \{(a, 0) \mid a \in \mathbb{R}\}.$$

Evident

$$(a, 0) \to a$$

este o bijecţie între mulţimea $\overline{\mathbb{R}}$ şi mulţimea $\mathbb{R}$ a numerelor reale. Mai mult, adunarea şi înmulţimea numerelor complexe dau pentru elementele mulţimii $\overline{\mathbb{R}}$ egalităţile

$$(a, 0) + (a', 0) = (a + a', 0),$$

$$(a, 0)(a', 0) = (aa', 0).$$

Aceste relații arată că regulile de adunare și înmulțire pe $\overline{\mathbb{R}}$ sînt aceleași ca cele de adunare și înmulțire a numerelor reale corespunzătoare. Astfel, submulțimea $\overline{\mathbb{R}}$ a lui $\mathbb{C}$ are aceleași proprietăți algebrice ca acelea ale mulțimii numerelor reale. Din acest motiv, putem identifica numărul complex $(a, 0)$ cu numărul real a, punînd $(a, 0) = a$. În particular, numerele complexe $(0, 0)$ și $(1, 0)$ sînt respectiv numerele reale 0 și 1.

Vom arăta acum că operațiile de adunare și înmulțire ale numerelor complexe au toate proprietățile fundamentale ale operațiilor de adunare și înmulțire de pe mulțimea numerelor reale (sau a numerelor raționale).

Teorema 1.1. *Operațiile de adunare și înmulțire a numerelor complexe au proprietățile:*

1) $\alpha + \alpha' = \alpha' + \alpha$, *oricare ar fi* $\alpha, \alpha' \in \mathbb{C}$ *(comutativitatea)*;

2) $\alpha + (\alpha' + \alpha'') = (\alpha + \alpha') + \alpha''$, *oricare ar fi* $\alpha, \alpha', \alpha'' \in \mathbb{C}$ *(asociativitatea)*;

3) $\alpha + 0 = 0 + \alpha = \alpha$, *oricare ar fi* $\alpha \in \mathbb{C}$;

4) *oricare ar fi* $\alpha \in \mathbb{C}$, *există* $\alpha^* \in \mathbb{C}$ *astfel încît*

$$\alpha + \alpha^* = \alpha^* + \alpha = 0;$$

5) $\alpha\alpha' = \alpha'\alpha$, *oricare ar fi* $\alpha, \alpha' \in \mathbb{C}$ *(comutativitatea)*;

6) $\alpha(\alpha'\alpha'') = (\alpha\alpha')\alpha''$, *oricare ar fi* $\alpha, \alpha', \alpha'' \in \mathbb{C}$ *(asociativitatea)*;

7) $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$, *oricare ar fi* $\alpha \in \mathbb{C}$;

8) *dacă* $\alpha \in \mathbb{C}$, $\alpha \neq 0$, *există* $\alpha^{**} \in \mathbb{C}$ *astfel încît*

$$\alpha\alpha^{**} = \alpha^{**}\alpha = 1;$$

9) $\alpha(\alpha' + \alpha'') = \alpha\alpha' + \alpha\alpha''$ și $(\alpha + \alpha')\alpha'' = \alpha\alpha'' + \alpha'\alpha''$, *oricare ar fi* $\alpha, \alpha', \alpha'' \in \mathbb{C}$ *(distributivitatea înmulțirii față de adunare)*.

Demonstrație. 1). Dacă $\alpha = (a, b)$, $\alpha' = (a', b')$, atunci

$$\alpha + \alpha' = (a, b) + (a', b') = (a + a', b + b') = \\ = (a' + a, b' + b) = (a', b') + (a, b) = \alpha' + \alpha.$$

2). Dacă $\alpha = (a, b), \alpha' = (a', b'), \alpha'' = (a'', b'')$, atunci

$$\alpha + (\alpha' + \alpha'') = (a, b) + [(a', b') + (a'', b'')] = \\ = (a, b) + (a' + a'', b' + b'') = (a + (a' + a''), b + (b' + b'')) = \\ = ((a + a') + a'', (b + b') + b'') = (a + a', b + b') + (a'', b'') = \\ = [(a, b) + (a', b')] + (a'', b'') = (\alpha + \alpha') + \alpha''.$$

3) Dacă $\alpha=(a, b)$, atunci $\alpha + 0 = (a, b) + (0, 0) = (a, b) = \alpha$. Evident şi $0 + \alpha = \alpha$.

4) Dacă $\alpha = (a, b)$, atunci $\alpha^* = (-a, -b)$ are proprietatea cerută, adică $\alpha + \alpha^* = (a, b) + (-a, -b) = (a - a, b - b) = (0, 0) = 0$.

Evident şi $\alpha^* + \alpha = 0$.

5) Dacă $\alpha = (a, b)$, $\alpha' = (a', b')$, atunci $\alpha\alpha' = (a, b)(a', b') = (aa'-bb', ab' + a'b) = (a'a-b'b, a'b + ab') = (a', b')(a, b) = \alpha'\alpha$.

6) Dacă $\alpha = (a, b)$, $\alpha' = (a', b')$, $\alpha'' = (a'', b'')$, atunci $\alpha(\alpha'\alpha'')=(a, b)[(a',b')(a'',b'')]=(a, b)(a'a''-b'b'', a'b''+a''b')=$
$$= (a(a'a'' - b'b'') - b(a'b'' + b'a''), a(a'b'' + b'a'') + b(a'a''-b'b'')) = ((aa'-bb')a''-(ab' + ba')b'', (aa'-bb')b'' + (ab' + ba')a'') = (aa'-bb', ab' + ba')(a'', b'') = (\alpha\alpha')\alpha''.$$

7) Dacă $\alpha = (a, b)$, atunci $\alpha\cdot 1 = (a, b)(1, 0) = (a, b) = \alpha$. Evident şi $1 \cdot \alpha = \alpha$.

8) Fie $\alpha = (a, b)$ nenul, adică $a^2 + b^2 \neq 0$. Dacă (x, y) este astfel încît $(a, b)(x, y) = (1, 0)$, atunci

$$(ax - by, ay + bx) = (1, 0).$$

De aici se obţine $ax - by = 1$; $bx + ay = 0$. Acest sistem are soluţia $x = \frac{a}{a^2 + b^2}$, $y = \frac{-b}{a^2 + b^2}$. Dar, evident, şi $(x, y)(a, b) = (1, 0)$, deci

$$\alpha^{**} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right).$$

9) Dacă $\alpha = (a, b)$, $\alpha' = (a', b')$, $\alpha'' = (a'', b'')$, atunci $\alpha(\alpha'+\alpha'')=(a, b)[(a', b') + (a'', b'')] = (a, b)(a'+a'', b'+b'') =$
$$= [a(a' + a'') - b(b' + b''), a(b' + b'') + b(a' + a'')] =$$
$$= (aa' + aa'' - bb' - bb'', ab' + ab'' + ba' + ba'') =$$
$$= [(aa'-bb') + (aa'' - bb''), (ab' + ba') + (ab'' + ba'')] =$$
$$= (aa'- bb', ab'+ba')+(aa''-bb'', ab''+ ba'') =$$
$$= (a, b)(a', b') + (a, b)(a'', b'') = \alpha\alpha' + \alpha\alpha''.$$

La fel se probează şi că $(\alpha + \alpha')\alpha'' = \alpha\alpha'' + \alpha'\alpha''$.

Definiţia 1.2. 1°. Numărul complex 0 se numeşte *element nul*.

2°. Dacă $\alpha \in \mathbb{C}$, numărul complex $\alpha^* \in \mathbb{C}$ astfel încît $\alpha + \alpha^* = \alpha^* + \alpha = 0$ se numeşte *opusul* lui α şi se notează cu $-\alpha$.

3°. Numărul complex 1 se numește *elementul unitate* al lui $\mathbb{C}$.

4°. Dacă $\alpha \in \mathbb{C}$, $\alpha \neq 0$, numărul complex $\alpha^{**} \in \mathbb{C}$ astfel încît $\alpha\alpha^{**} = \alpha^{**}\alpha = 1$ se numește *inversul* lui α și se notează cu α^{-1}.

Numărul complex (0, 1) are proprietatea că $(0, 1)(0, 1) = (-1, 0) = -1$, deci este o rădăcină a ecuației $x^2 + 1 = 0$. Așadar, această ecuație are soluții în mulțimea numerelor complexe, ceea ce nu este posibil în mulțimea numerelor reale.

Convenim să notăm prin simbolul i numărul complex (0, 1).

Să arătăm acum că numerele complexe introduse se pot reprezenta sub forma obișnuită, care va fi folosită în cele ce urmează.

Fie $\alpha = (a, b) \in \mathbb{C}$. Avînd în vedere cele de mai sus, avem

$$\alpha = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + b\mathrm{i}.$$

În mod tradițional, vom numi *unitate imaginară* numărul complex i; numerele de forma bi se numesc *imaginare.* Dacă numărul complex α se scrie $\alpha = a + b\mathrm{i}$, atunci a se numește *partea reală*, iar bi *partea imaginară* a numărului α.

Reluăm adunarea și înmulțirea a două numere complexe reprezentate sub această ultimă formă. Astfel, se obține

$$\alpha + \alpha' = (a + b\mathrm{i}) + (a' + b'\mathrm{i}) = (a, b) + (a', b') = $$
$$= (a + a', b + b') = (a + a') + (b + b')\mathrm{i};$$

$$\alpha\alpha' = (a + b\mathrm{i})(a' + b'\mathrm{i}) = (a, b)(a', b') = (aa' - bb', ab' + a'b) =$$
$$= (aa' - bb') + (ab' + a'b)\mathrm{i}.$$

Observăm că $\mathrm{i}^2 = -1$, $\mathrm{i}^3 = -\mathrm{i}$, $\mathrm{i}^4 = 1$ și, mai general, avem egalitățile

$$\mathrm{i}^{4k} = 1, \quad \mathrm{i}^{4k+1} = \mathrm{i}, \quad \mathrm{i}^{4k+2} = -1, \quad \mathrm{i}^{4k+3} = -\mathrm{i},$$

k fiind un număr natural oarecare.

§ 2. Reprezentarea geometrică a numerelor complexe

Fie (Δ) o dreaptă pe care fixăm o origine O și fie de asemenea u o unitate de măsură. Dacă facem să-i corespundă oricărui punct al dreptei (Δ) abscisa sa se obține o corespondență bijec-

tivă între punctele acestei drepte şi numerele reale. Această corespondenţă dă o reprezentare geometrică a numerelor reale prin punctele unei drepte.

Fie un plan (ω) în care este fixat un sistem de axe rectangulare xOy. În acest plan numărul complex $\alpha = (a, b)$ se reprezintă prin punctul A de coordonate a şi b (a fiind abscisa iar b ordonata sa).

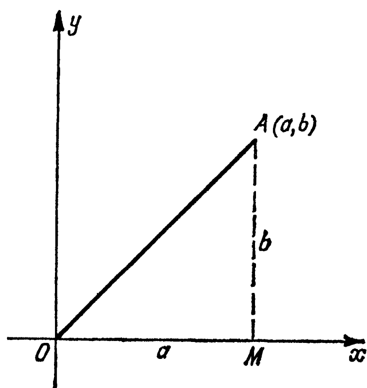


Fig. 1

Punctul $A(a, b)$ se mai numeşte şi *afixul* numărului complex $\alpha = a + bi$.

Asocierea

$$\alpha = a + bi \to A(a, b)$$

este o funcţie bijectivă de la mulţimea numerelor complexe în planul (ω). Prin aceasta, mulţimii numerelor reale îi corespunde axa Ox iar mulţimii numerelor imaginare îi corespunde axa Oy. De aceea axa Ox se numeşte *axa reală* iar axa Oy se numeşte *axa imaginară* a planului (ω).

Planul ale cărui puncte se identifică cu numerele complexe se numeşte *planul complex*.

Reprezentarea numerelor complexe în plan pune în mod natural problema interpretării geometrice a operaţiilor algebrice definite în mulţimea numerelor complexe.

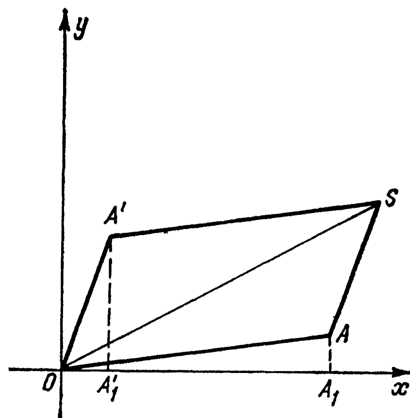


Fig. 2

Să dăm mai întîi interpretarea geometrică a adunării.

Fie două numere $\alpha = a + bi$ şi $\alpha' = a' + b'i$ ale căror afixe sînt A şi A'. Atunci numărul complex al cărui afix S este al patrulea vîrf al paralelogramului, care are celelalte trei vîrfuri respectiv A, O şi A', reprezintă suma $\alpha + \alpha' = (a + a') + (b + b')i$.

Pentru a da interpretarea geometrică a înmulţirii, vom introduce mai întîi reprezentarea trigonometrică a numerelor complexe. Cînd scriem un număr complex α sub forma $a + bi$, se folosesc coordonatele carteziene ale afixului A al numărului α.

În scrierea trigonometrică a numerelor complexe se folosesc coordonatele polare ale afixului A, corespunzător, adică distanţa ρ a punctului A la origine şi unghiul φ pe care raza vectoare OA îl formează cu sensul pozitiv al axei absciselor. Numărul ρ care este real şi pozitiv se numeşte *modulul* lui α şi se notează prin $|\alpha|$. Observăm că $\rho = 0$ dacă şi numai dacă A coincide cu originea. Dacă A este pe axa reală, adică dacă numărul α este real, atunci ρ este valoarea absolută sau modulul numărului α.

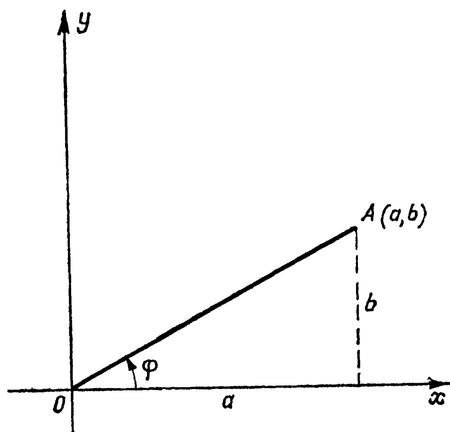


Fig. 3

Unghiul φ se numeşte *argumentul* lui α şi se notează prin arg α. Argumentul este definit în afara unui multiplu de 2π. Argumentul numărului 0 nu este definit, dar acest număr este bine determinat prin egalitatea $|0| = 0$.

Legătura între coordonatele polare şi carteziene este dată de egalităţile următoare:

$$a = \rho \cos \varphi, \; b = \rho \sin \varphi.$$

De aici se obţine evident

$$\rho = +\sqrt{a^2 + b^2}.$$

Aceste formule dau *forma trigonometrică* a unui număr complex $\alpha = a + bi$ şi anume

$$\alpha = \rho\,(\cos \varphi + i \sin \varphi).$$

Mai mult, în mod evident, această reprezentare este unică.

Fie două numere complexe α şi α' date sub formă trigonometrică

$$\alpha = \rho(\cos \varphi + i \sin \varphi), \; \alpha' = \rho'(\cos \varphi' + i \sin \varphi').$$

Calculăm produsul lor

$$\alpha\alpha' = [\rho(\cos\varphi + i\sin\varphi)]\,[\rho'(\cos\varphi' + i\sin\varphi')] =$$
$$= \rho\rho'(\cos\varphi\cos\varphi' + i\cos\varphi\sin\varphi' + i\sin\varphi\cos\varphi - \sin\varphi\sin\varphi') =$$
$$= \rho\rho'[(\cos\varphi\cos\varphi' - \sin\varphi\sin\varphi') + i(\sin\varphi\cos\varphi' + \cos\varphi\sin\varphi')]$$

Deci

$$\alpha\alpha' = \rho\rho'\,[\cos(\varphi + \varphi') + i\sin(\varphi + \varphi')].$$

De aici, se deduce că *modulul produsului a două numere complexe este egal cu produsul modulelor factorilor*, adică

$$|\alpha\alpha'| = |\alpha|\,|\alpha'|.$$

De asemenea, *argumentul produsului a două numere complexe este egal cu suma argumentelor factorilor*, adică

$$\arg(\alpha\alpha') = \arg\alpha + \arg\alpha'.$$

Aceste reguli se extind la un număr finit de factori. Într-adevăr, fie $\alpha_1, \alpha_2, \ldots, \alpha_n$ numere complexe care sub formă trigonometrică se scriu astfel :

$$\alpha_k = \rho_k(\cos\varphi_k + i\sin\varphi_k),\ k = 1, 2, \ldots, n.$$

Să demonstrăm formula

$$\prod_{k=1}^{n}\alpha_k = \prod_{k=1}^{n}\rho_k\left(\cos\sum_{k=1}^{n}\varphi_k + i\sin\sum_{k=1}^{n}\varphi_k\right).$$

Vom demonstra aceasta prin inducție matematică după n. Pentru $n = 2$ formula este verificată, după cum am arătat mai înainte. Să presupunem acum că aceasta este adevărată pentru $n - 1$ factori și să o demonstrăm pentru n factori. Așadar, dacă

$$\prod_{k=1}^{n-1}\alpha_k = \prod_{k=1}^{n-1}\rho_k\left(\cos\sum_{k=1}^{n-1}\varphi_k + i\sin\sum_{k=1}^{n-1}\varphi_k\right),$$

atunci

$$\prod_{k=1}^{n} \alpha_k = \left(\prod_{k=1}^{n-1} \alpha_k\right) \alpha_n =$$

$$= \left[\prod_{k=1}^{n-1} \rho_k \left(\cos \sum_{k=1}^{n-1} \varphi_k + i \sin \sum_{k=1}^{n-1} \varphi_k\right)\right] \left[\rho_n(\cos \varphi_n + i \sin \varphi_n)\right] =$$

$$= \left(\prod_{k=1}^{n-1} \rho_k\right) \rho_n \left[\cos \left(\sum_{k=1}^{n-1} \varphi_k + \varphi_n\right) + i \sin \left(\sum_{k=1}^{n-1} \varphi_k + \varphi_n\right)\right] =$$

$$= \prod_{k=1}^{n} \rho_k \left(\cos \sum_{k=1}^{n} \varphi_k + i \sin \sum_{k=1}^{n} \varphi_k\right).$$

Rezultă

$$\left|\prod_{k=1}^{n} \alpha_k\right| = \prod_{k=1}^{n} |\alpha_k| \text{ şi } \arg \left(\prod_{k=1}^{n} \alpha_k\right) = \sum_{k=1}^{n} \arg \alpha_k.$$

Dacă $\alpha_k = \alpha = \rho\,(\cos \varphi + i \sin \varphi)$, $k = 1, 2, \ldots, n$, atunci

$$\alpha^n = \rho^n\,(\cos n\varphi + i \sin n\varphi),$$

n fiind un număr natural oarecare. Această egalitate este cunoscută sub denumirea de *formula lui Moivre*. Astfel, *pentru a ridica un număr complex la puterea a n-a ridicăm la puterea a n-a modulul său şi multiplicăm cu n argumentul său.*

Iată o aplicaţie a acestui fapt. Dacă $\rho = 1$, atunci se obţine

$$(\cos \varphi + i \sin \varphi)^n = \cos n\varphi + i \sin n\varphi$$

care permite obţinerea expresiilor lui $\sin n\varphi$ şi $\cos n\varphi$ în funcţie de puterile lui $\sin \varphi$ şi $\cos \varphi$. Într-adevăr, dacă dezvoltăm primul membru al acestei egalităţi şi separăm partea reală şi imaginară, deducem

$$\cos n\varphi = \cos^n \varphi - C_n^2 \cos^{n-2} \varphi \sin^2 \varphi + C_n^4 \cos^{n-4} \varphi \sin^4 \varphi - \ldots,$$

$$\sin n\varphi = C_n^1 \cos^{n-1} \varphi \sin \varphi - C_n^3 \cos^{n-3} \varphi \sin^3 \varphi +$$
$$+ C_n^5 \cos^{n-5} \varphi \sin^5 \varphi - \ldots,$$

unde

$$C_n^k = \frac{n(n-1)\dots(n-k+1)}{1\cdot 2\cdot \dots \cdot k}.$$

Fie α şi α' două numere complexe care au afixele A şi A'. Atunci produsul celor două numere complexe este un număr complex al cărui afix P se obţine astfel: se roteşte raza vectoare OA în sens direct (invers acelor unui ceasornic) cu un unghi $\varphi' = \arg \alpha'$ şi apoi se multiplică acest vector de $\rho' = |\alpha'|$ ori.

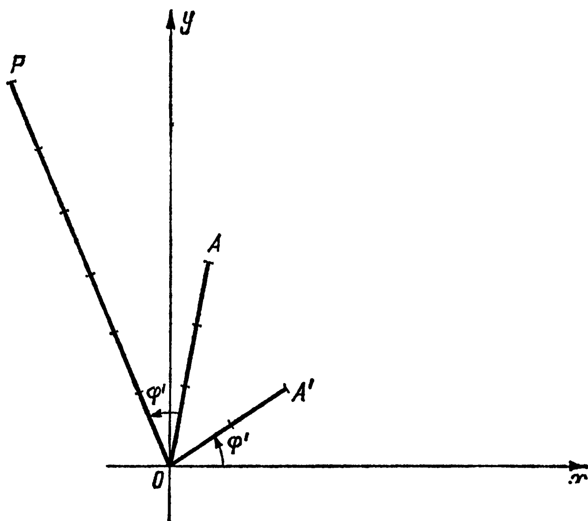


Fig. 4

Fie $\alpha=\rho(\cos\varphi+i \sin \varphi)$ un număr complex nenul. Atunci

$$\alpha^{-1} = \frac{1}{\alpha} = \frac{1}{\rho(\cos\varphi + i\sin\varphi)} = \frac{1}{\rho}\cdot\frac{\cos\varphi - i\sin\varphi}{\cos^2\varphi + \sin^2\varphi} =$$
$$= \rho^{-1}[\cos(-\varphi) + i\sin(-\varphi)].$$

Deci $|\alpha^{-1}| = |\alpha|^{-1}$ şi $\arg \alpha^{-1} = -\arg \alpha$.

Aşadar, dacă A este afixul numărului complex α, atunci afixul A_1 al numărului complex α^{-1} se obţine astfel: pe semidreapta OA se consideră punctul A' care se găseşte la distanţa ρ^{-1} de O şi apoi se ia simetricul său A_1 faţă de axa reală.

Rezultă că dacă $\alpha = \rho(\cos\varphi + i\sin\varphi)$ şi $\alpha' = \rho'(\cos\varphi' + i\sin\varphi') \neq 0$, atunci $\frac{\alpha}{\alpha'} = \alpha(\alpha')^{-1} = \rho(\rho')^{-1}(\cos(\varphi - \varphi') + i\sin(\varphi - \varphi'))$. Deci $\left|\frac{\alpha}{\alpha'}\right| = \frac{|\alpha|}{|\alpha'|}$ şi $\arg\frac{\alpha}{\alpha'} = \arg\alpha - \arg\alpha'$.

Propoziţia 2.1. *Oricare ar fi numerele complexe α şi α' au loc inegalităţile :*

$$|\alpha| - |\alpha'| \leqslant |\alpha + \alpha'| \leqslant |\alpha| + |\alpha'|,$$

$$|\alpha| - |\alpha'| \leqslant |\alpha - \alpha'| \leqslant |\alpha| + |\alpha'|.$$

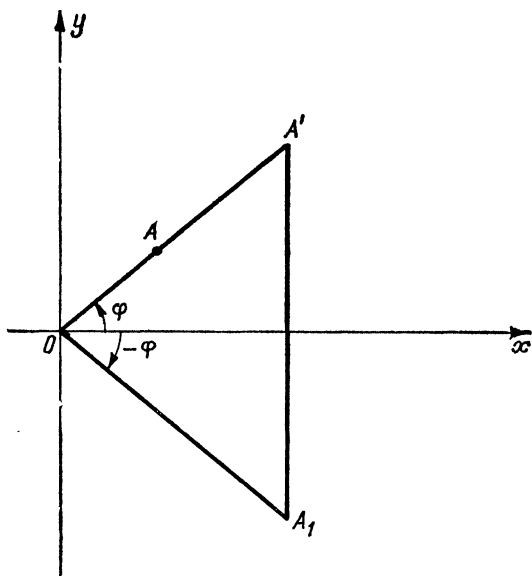


Fig. 5

Demonstraţie. Observăm mai întîi că al doilea şir de inegalităţi se obţine din primul, dacă scriem $\alpha - \alpha' = \alpha + (-\alpha')$ şi ţinem seama de faptul că $|-\alpha'| = |\alpha'|$. Aşadar, să demonstrăm primul şir de inegalităţi.

Fie $\alpha = \rho(\cos\varphi + i\sin\varphi)$ şi $\alpha' = \rho'(\cos\varphi' + i\sin\varphi')$ şi fie $\alpha + \alpha' = s(\cos\bar{\varphi} + i\sin\bar{\varphi})$, de unde

$$\rho\cos\varphi + \rho'\cos\varphi' = s\cos\bar{\varphi},$$

$$\rho\sin\varphi + \rho'\sin\varphi' = s\sin\bar{\varphi}.$$

Dacă înmulţim ambii membri ai primei egalităţi cu $\cos\bar{\varphi}$ iar pe cei din a doua cu $\sin\bar{\varphi}$ şi apoi îi adunăm parte cu parte, se obţine

$$\rho(\cos\varphi\cos\bar{\varphi} + \sin\varphi\sin\bar{\varphi}) + \rho'(\cos\varphi'\cos\bar{\varphi} + \sin\varphi'\sin\bar{\varphi}) = s(\cos^2\bar{\varphi} + \sin^2\bar{\varphi}),$$

adică

$$\rho\cos(\varphi - \bar{\varphi}) + \rho'\cos(\varphi - \bar{\varphi}) = s.$$

Dar $s = \rho \cos(\varphi - \bar{\varphi}) + \rho' \cos(\varphi' - \bar{\varphi}) \leqslant \rho + \rho'$ (deoarece cosinusul unui unghi este mai mic ca 1) şi deci $|\alpha + \alpha'| \leqslant \leqslant |\alpha| + |\alpha'|$. Apoi

$$\alpha = (\alpha + \alpha') - \alpha' = (\alpha + \alpha') + (-\alpha')$$

şi deci

$$|\alpha| = |(\alpha + \alpha') + (-\alpha')| \leqslant |\alpha + \alpha'| + |-\alpha'| = |\alpha + \alpha'| + |\alpha'|.$$

Aşadar $|\alpha| - |\alpha'| \leqslant |\alpha + \alpha'|$. Deci, am demonstrat că

$$|\alpha| - |\alpha'| \leqslant |\alpha + \alpha'| \leqslant |\alpha| + |\alpha'|.$$

Definiţie. Se numeşte *conjugatul* unui număr complex $\alpha = a + bi$ numărul complex $\bar{\alpha} = a - bi$.

Deoarece afixele numerelor complexe α şi $\bar{\alpha}$ sînt simetrice faţă de axa reală, rezultă că $|\bar{\alpha}| = |\alpha|$ şi $\arg \alpha = -\arg \bar{\alpha}$.

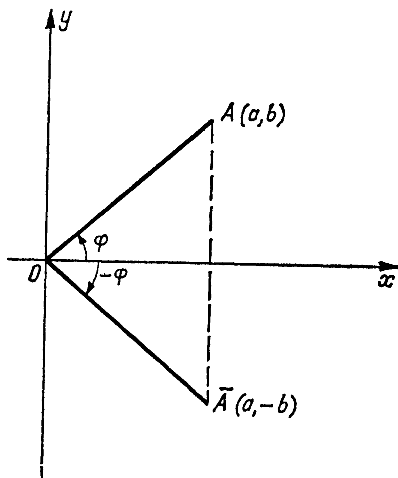


Fig. 6

Suma şi produsul a două numere complexe conjugate sînt numere reale. Într-adevăr,

$$\alpha + \bar{\alpha} = 2a,$$
$$\alpha\bar{\alpha} = a^2 + b^2 = |\alpha|^2.$$

Remarcăm că ultima egalitate arată că dacă $\alpha \neq 0$, atunci $\alpha\bar{\alpha}$ este pozitiv.

Dacă $\alpha = a + bi$ şi $\alpha' = a' + b'i$, avem de asemenea în mod evident relaţiile :

$$(a - bi) + (a' - b'i) = (a + a') - (b + b')i$$

şi

$$(a - bi)(a' - b'i) = (aa' - bb') - (ab' + a'b)i$$

sau

$$\overline{\alpha + \alpha'} = \bar{\alpha} + \bar{\alpha}', \quad \overline{\alpha\alpha'} = \bar{\alpha}\bar{\alpha}'.$$

Deci, numărul complex conjugat al sumei (produsului) a două numere complexe este suma (produsul) numerelor complexe conjugate ale fiecărui termen (factor) al sumei (produsului).

§ 3. Extragerea rădăcinii dintr-un număr complex. Rădăcinile unității

Fie n un număr natural și α un număr complex oarecare. Un număr complex β astfel încît $\beta^n = \alpha$ se numește *rădăcină de ordin n* a numărului α. Problema aflării rădăcinii de un anumit ordin dintr-un număr complex comportă, în general, dificultăți mari. Dar, folosind forma trigonometrică a numerelor complexe, este ușor de rezolvat complet această chestiune. Deocamdată, nu ne punem problema dacă este posibil să facem acest lucru și să presupunem că fiind dat un număr complex $\alpha = \rho(\cos\varphi + i\sin\varphi)$, există un număr complex $\beta = r(\cos\theta + i\sin\theta)$ astfel încît $\beta^n = \alpha$. Ne propunem să aflăm numărul β. Avem

$$[r(\cos\theta + i\sin\theta)]^n = \rho(\cos\varphi + i\sin\varphi)$$

sau, aplicînd formula lui Moivre

$$r^n(\cos n\theta + i\sin n\theta) = \rho(\cos\varphi + i\sin\varphi),$$

de unde $r^n = \rho$, $n\theta = \varphi + 2k\pi$, cu $k \in \mathbb{Z}$. Deci $r = \sqrt[n]{\rho}$, acesta fiind numărul real pozitiv bine determinat, astfel încît $r^n = \rho$ (ρ fiind de asemenea real și pozitiv), iar

$$\theta = \frac{\varphi + 2k\pi}{n}.$$

Mai mult, dacă $k \in \mathbb{Z}$, atunci numărul $\beta_k = \sqrt[n]{\rho}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right)$ ridicat la puterea a n-a va da α și deci, oricare ar fi $k \in \mathbb{Z}$, aceste numere sînt rădăcini de ordinul n ale lui α. Dar cum $\cos\varphi$ și $\sin\varphi$ sînt funcții trigonometrice periodice, de perioadă 2π, se obțin numai n rădăcini distincte de ordinul n ale lui α. Într-adevăr, dacă k este un număr întreg oarecare, după teorema împărțirii cu rest avem $k = nq + r$, unde r și q sînt numere întregi, iar $0 \leqslant r \leqslant n - 1$. Atunci

$$\frac{\varphi + 2k\pi}{n} = \frac{\varphi + 2(nq + r)\pi}{n} = \frac{\varphi + 2r\pi}{n} + 2q\pi,$$

de unde $\beta_k = \beta_r$. Așadar, se obțin doar n rădăcini distincte și anume $\beta_0, \beta_1, \ldots, \beta_{n-1}$.

Cum toate cele n rădăcini au modulul egal cu $\sqrt[n]{\rho}$, rezultă că afixele lor se găsesc pe un cerc cu centrul în origine de rază $\sqrt[n]{\rho}$. Mai mult, deoarece argumentele celor n rădăcini sînt în progresie aritmetică cu rația $\frac{2\pi}{n}$, rezultă că afixele celor n rădăcini de ordinul n ale unui număr complex de modul ρ sînt vîrfurile unui poligon regulat cu n laturi înscris în cercul cu centrul în origine și de rază $\sqrt[n]{\rho}$.

În particular, rădăcinile de ordinul n ale unității sînt rădăcinile de ordinul n ale numărului $\alpha=1 = \cos 0 + i \sin 0$, adică

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ k = 0, 1, \ldots, n-1.$$

Să notăm cu $U_n = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\}$ mulțimea acestor rădăcini.

Exemple. 1. Rădăcinile de ordinul doi ale unității sînt ± 1, deci $U_2 = \{-1, 1\}$.

2. Rădăcinile cubice (de ordinul trei) ale unității sînt

$$\varepsilon_0 = \cos 0 + i\sin 0 = 1;$$

$$\varepsilon_1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2};$$

$$\varepsilon_2 = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

3. Rădăcinile de ordinul 4 ale unității sînt ± 1, $\pm i$, deci $U_4 = \{-1, 1, -i, i\}$.

Propoziția 3.1. *Dacă α este un număr complex oarecare, orice rădăcină de ordinul n a lui α se obține multiplicînd una dintre acestea prin toate rădăcinile de ordinul n ale unității.*

Demonstrație. Fie β o rădăcină de ordinul n a lui α, adică $\beta^n = \alpha$, și fie ε o rădăcină oarecare a unității, adică $\varepsilon^n = 1$. Atunci $(\beta\varepsilon)^n = \beta^n\varepsilon^n = \alpha$, deci $\beta\varepsilon$ este de asemenea o rădăcină de ordinul n a lui α. Întrucît $\beta\varepsilon_0, \beta\varepsilon_1, \ldots, \beta\varepsilon_{n-1}$ sînt n rădăcini distincte ale lui α, rezultă că acestea sînt toate rădăcinile de ordinul n ale lui α.

O b s e r v a ț i e. Mulțimea U_n a rădăcinilor de ordinul n ale unității față de înmulțirea obișnuită a numerelor complexe are unele proprietăți pe care le semnalăm în cele ce urmează.

Dacă ε și σ sînt două astfel de rădăcini, adică $\varepsilon^n = 1$ și $\sigma^n = 1$, atunci $(\varepsilon\sigma)^n = \varepsilon^n \cdot \sigma^n = 1$ și deci produsul lor este de asemenea o rădăcină de ordinul n a unității. Deci, dacă $\varepsilon, \sigma \in U_n$, atunci $\varepsilon\sigma \in U_n$. Înmulțirea este evident asociativă și comutativă. Rădăcina $1 \in U_n$ este element neutru la înmulțire. În sfîrșit, dacă $\varepsilon \in U_n$, adică $\varepsilon^n = 1$, atunci $(\varepsilon^{-1})^n = \varepsilon^{-n} = \frac{1}{\varepsilon^n} = 1$ și deci $\varepsilon^{-1} \in U_n$, fiind inversa lui ε.

Fie din nou $U_n = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\}$ mulțimea rădăcinilor de ordinul n ale unității și

$$\varepsilon = \varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Toate celelalte rădăcini sînt o putere a lui ε, mai precis:

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^k.$$

Deci, rădăcinile de ordinul n ale unității sînt

$$\varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}, \varepsilon^n = 1.$$

Definiția 3.1. O rădăcină de ordinul n a unității, astfel încît orice altă rădăcină de ordinul n a unității este o putere a sa, se numește *rădăcină primitivă* de ordinul n a unității.

Deci ε este o astfel de rădăcină primitivă, dacă

$$U_n = \{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}\}.$$

Numărul ε nu este singura rădăcină primitivă, după cum vom vedea în cap. II, §6.

II

ELEMENTE DE STRUCTURI ALGEBRICE

§ 1. Noţiunea de operaţie algebrică internă

Definiţia 1.1. Fie M o mulţime. Se numeşte *operaţie algebrică* sau *lege de compunere internă*, definită pe M, orice funcţie u definită pe $M \times M$ cu valori în M:

$$u : M \times M \to M, \ (x, y) \to u(x, y).$$

Pentru că în cele ce urmează nu intervin decît operaţii algebrice interne vom spune, pe scurt, *operaţie algebrică* în loc de operaţie algebrică internă.

Exemple. 1. Pe mulţimile de numere $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ adunarea şi înmulţirea sînt operaţii algebrice.

2. Pe mulţimea $\mathbb{Z}$ a numerelor întregi scăderea este o operaţie algebrică. Ea este definită astfel:

$$s : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \ s(x, y) = x + (-y) = x - y.$$

De asemenea, scăderea este operaţie algebrică şi pe $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Însă, pe mulţimea $\mathbb{N}$ a numerelor naturale scăderea nu este operaţie algebrică, deoarece rezultatul acesteia nu este întotdeauna un număr natural.

3. Fie M o mulţime. Pe mulţimea

$$\mathcal{F}(M) = \{f \mid f : M \to M\}$$

a tuturor funcţiilor de la M la M definim următoarea operaţie algebrică. Dacă $f, g \in \mathcal{F}(M)$, atunci funcţia $h : M \to M$, definită prin

$$h(x) = g(f(x)),$$

se numeşte *compunerea* lui g cu f şi se notează $g \circ f$, sau uneori, chiar gf.

În cele ce urmează apar numeroase exemple de operaţii algebrice. Deoarece nu vom lucra şi cu alte tipuri de operaţii, vom spune, uneori, simplu, *operaţie* în loc de operaţie algebrică. Vom nota pentru orice operaţie algebrică $u : M \times M \to M$ elementul $u(x, y)$ corespunzător perechii (x, y) prin $x * y$, sau, după caz, xy (notaţie multiplicativă) sau $x + y$ (notaţie aditivă).

Dăm cîteva proprietăţi ale operaţiilor algebrice, cu ajutorul cărora se definesc structurile de bază ale algebrei.

— *Asociativitatea.* Fie M o mulţime şi $* : M \times M \to M$ o operaţie pe mulţimea M. Se spune că operaţia $*$ este *asociativă*, dacă oricare ar fi elementele x, y, z din M, are loc egalitatea

$$x * (y * z) = (x * y) * z.$$

Exemple. Adunarea şi înmulţirea pe $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sînt operaţii asociative. De asemenea compunerea funcţiilor pe $\mathcal{F}(M)$ este evident o operaţie asociativă. Însă, scăderea numerelor nu este operaţie asociativă. De exemplu :

$$5-(4-7)=8 \text{ iar } (5-4)-7=-6.$$

— *Comutativitatea.* Spunem că o operaţie $*$ definită pe o mulţime M este *comutativă* dacă, oricare ar fi elementele x, y din M, are loc egalitatea

$$x * y = y * x.$$

Exemple. Adunarea şi înmulţirea pe $\mathbb{N}$. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sînt operaţii comutative, în timp ce scăderea nu este comutativă. Compunerea funcţiilor pe $\mathcal{F}(M)$, în general, nu este comutativă. Se poate arăta cu uşurinţă că compunerea funcţiilor pe $\mathcal{F}(M)$ este comutativă dacă şi numai dacă M are cel mult un element. Lăsăm, ca exerciţiu, cititorului verificarea acestei afirmaţii.

— *Element neutru.* Se spune că elementul $e \in M$ este *element neutru* (*unitate*) pentru operaţia $* : M \times M \to M$ dacă, oricare ar fi $x \in M$, avem

$$x * e = e * x = x.$$

Numărul 0 este element neutru pentru adunarea în $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, în timp ce 1 este element neutru pentru înmulţire. Pentru compunerea funcţiilor pe M funcţia identică 1_M este element neutru.

Dacă considerăm mulţimea $2\mathbb{Z}$ a numerelor întregi pare, înmulţirea numerelor întregi pe această mulţime este o operaţie algebrică care evident nu are element neutru.

Pentru o operaţie algebrică care are element neutru are loc :

Propoziţia 1.1. *Pentru orice operaţie algebrică, elementul neutru (dacă există) este unic.*

Demonstraţie. Să presupunem că operaţia $*$ are două elemente neutre e şi e' şi să arătăm că $e = e'$. Deoarece e este element neutru, rezultă $e * e' = e'$, iar cum e' este element neutru, rezultă $e * e' = e$ şi deci $e = e'$.

Elementul neutru se mai numeşte şi *element unitate* atunci cînd operaţia este notată multiplicativ şi *element zero* (*nul*) cînd operaţia este notată aditiv.

— *Elemente inversabile.* Fie $*$ o operaţie algebrică pe M cu element neutru e şi $x \in M$. Spunem că x este *simetrizabil* în raport cu operaţia dată, dacă există un element $x' \in M$ astfel încît

$$x * x' = x' * x = e.$$

Elementul x' se numeşte *simetricul* lui x. În notaţia multiplicativă a operaţiei algebrice, x' se mai numeşte *inversul* lui x, iar în cea aditivă, *opusul* lui x.

Propoziţia 1.2. *Fie* $* : M \times M \to M$ *o operaţie asociativă şi cu element neutru* e. *Dacă elementul* $x \in M$ *este inversabil, atunci inversul său* x' *este unic.*

Demonstraţie. Fie x' şi x'' două elemente din M astfel încît $x * x' = x' * x = e$ şi $x * x'' = x'' * x = e$. Avem $x'' * (x * x') = x'' * e = x''$. Pe de altă parte $x'' * (x * x') = (x'' * x) * x' = e * x' = x'$. Deci $x' = x''$.

Notăm inversul elementului $x \in M$ prin x^{-1}. Cînd operaţia este aditivă, notăm opusul lui x prin $-x$.

Referindu-ne la exemplele de operaţii de mai sus, observăm că în raport cu adunarea în $\mathbb{Z}$, opusul numărului n este $-n$; în raport cu înmulţirea în $\mathbb{Z}$ elementele inversabile sînt 1 şi -1, iar toate celelalte numere întregi sînt neinversabile. Cînd ope-

rația nu are element neutru, pentru aceasta nu se poate pune problema elementelor simetrizabile.

În ceea ce privește compunerea funcțiilor, demonstrăm

Propoziția 1.3. *O funcție $f : M \to N$ este inversabilă dacă și numai dacă este bijectivă.*

Demonstrație. Fie $f : M \to N$ inversabilă, adică există $g : N \to M$ astfel încît $f \circ g = 1_N$ și $g \circ f = 1_M$. Să arătăm că f este bijectivă. Într-adevăr, dacă $f(x) = f(x')$, atunci $g(f(x)) = g(f(x'))$ și deci $(g \circ f)(x) = (g \circ f)(x')$, adică $1_M(x) = 1_M(x')$, de unde $x = x'$. Așadar, funcția f este injectivă. Pentru a demonstra surjectivitatea funcției f, fie $y \in N$. Deoarece $y = 1_N(y) = (f \circ g)(y) = f(g(y))$, rezultă că f este surjectivă. Fie f bijectivă. Definim $g : N \to M$ în modul următor. Dacă $y \in N$, iar f este surjectivă, există $x \in M$ astfel încît $f(x) = y$. Cum f este injectivă, x este unic cu această proprietate. Punem atunci $g(y) = x$, unde $f(x) = y$. Evident g este o funcție astfel încît $g \circ f = 1_M$ și $f \circ g = 1_N$.

După această propoziție rezultă că elementele inversabile din $\mathcal{F}(M)$ în raport cu compunerea funcțiilor sînt funcțiile bijective.

Propoziția 1.4. *Fie M o mulțime înzestrată cu operația $*$ și care admite element neutru e. Dacă $x, y \in M$ sînt inversabile, atunci $x * y$ este inversabil și*

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Demonstrație. Cum $(x * y)*(y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} = x * x^{-1} = e$ și, analog, $(y^{-1} * x^{-1}) * (x * y) = e$, rezultă $(x * y)^{-1} = y^{-1} * x^{-1}$.

§ 2. Grup, subgrup, omomorfisme de grupuri

Definiția 2.1. Se numește *grup* o mulțime nevidă G înzestrată cu o operație algebrică $* : G \times G \to G$, asociativă, cu element neutru și astfel încît orice element din G este simetrizabil.

Se mai spune că, în acest caz, pe G s-a dat o *structură de grup*. Dacă, în plus, operația este comutativă, spunem că grupul este *comutativ* sau *abelian*.

În general, într-un grup oarecare G, elementul $x * y$ se notează xy şi se numeşte *produsul* lui x cu y sau cu $x + y$ şi se numeşte *suma* lui x cu y. După caz, se spune că grupul G este multiplicativ sau aditiv.

Exemple. 1. Mulţimile $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ şi $\mathbb{C}$ sînt grupuri comutative în raport cu operaţia de adunare corespunzătoare fiecăreia dintre acestea.

2. $\mathbb{C}^* = \{\alpha \in \mathbb{C} | \alpha \neq 0\}$ (mulţimea numerelor complexe nenule) cu operaţia de înmulţire este un grup comutativ. Analog, $\mathbb{Q}^*$, $\mathbb{R}^*$.

3. $\mathbb{R}^*_+ = \{x \in \mathbb{R} | x > 0\}$, mulţimea numerelor reale pozitive, înzestrată cu operaţia de înmulţire este grup comutativ. Analog, $\mathbb{Q}^*_+$.

4. Mulţimea $G = \{1, -1\} \subset \mathbb{Z}$ pe care este definită operaţia de înmulţire a numerelor întregi este un grup comutativ.

5. Mulţimea $U_n = \{z \in \mathbb{C} | z^n = 1\}$, $n \geqslant 1$, este un grup comutativ faţă de înmulţirea numerelor complexe (vezi observaţia din § 3, cap. I). Acesta este grupul rădăcinilor de ordinul n ale unităţii.

6. Fie $\sigma(M) = \{f: M \to M | f \text{ bijectivă}\}$. Deoarece o funcţie este bijectivă dacă şi numai dacă este inversabilă (vezi propoziţia 1.3) iar compunerea a două funcţii inversabile este inversabilă (vezi propoziţia 1.4), rezultă că compunerea funcţiilor pe $\sigma(M)$ este o operaţie algebrică împreună cu care $\sigma(M)$ este grup, în general, necomutativ.

Lăsăm ca exerciţiu să se arate că $\sigma(M)$ este comutativ dacă şi numai dacă M are cel mult două elemente.

Definiţia 2.2. O submulţime nevidă H a unui grup G se spune că este un *subgrup* al lui G dacă operaţia algebrică de pe G induce pe H o operaţie algebrică împreună cu care H este grup.

Propoziţia 2.1. *Fie G un grup şi H o submulţime nevidă a sa. Atunci următoarele afirmaţii sînt echivalente:*

1) *H este subgrup al lui G.*

2) *Sînt satisfăcute următoarele condiţii:*

   1° *Pentru orice $x, y \in H$ rezultă $xy \in H$.*

   2° *$e \in H$ (e fiind elementul neutru al lui G).*

   3° *Pentru orice $x \in H$ rezultă $x^{-1} \in H$.*

3) *Pentru orice $x, y \in H$ rezultă $xy^{-1} \in H$.*

Demonstraţie. 1) $\Rightarrow$ 2). Cum operaţia de pe G induce o operaţie pe H, rezultă că pentru orice $x, y \in H$ avem $xy \in H$, adică condiţia 1°. Fie e' elementul neutru al lui H. Atunci avem $e'e' = e'$ şi dacă $(e')^{-1}$ este inversul lui e' în G, atunci $e' = (e')(e')^{-1} = e$ şi deci $e \in H$, adică condiţia 2°. Fie $x \in H$ şi x' inversul lui x în H. Cum e este elementul neutru al lui H, atunci $xx' = x'x = e$, deci x' este inversul lui x în G, adică $x' = x^{-1}$. Aşadar $x^{-1} \in H$, adică 3°.

2) $\Rightarrow$ 3). Dacă $x, y \in H$, conform cu 3° rezultă $y^{-1} \in H$ și după 1°, $xy^{-1} \in H$.

3) $\Rightarrow$ 1). Dacă $x \in H$, atunci $xx^{-1} = e \in H$ și $x^{-1} = ex^{-1} \in H$. De asemenea, dacă $y \in H$ și cum $y^{-1} \in H$, se obține

$$xy = x(y^{-1})^{-1} \in H.$$

De exemplu $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sînt subgrupuri unul în celălalt față de operația de adunare. Grupul $\mathbb{R}^*_+$ este subgrup al lui $\mathbb{R}^*$; $\{1, -1\}$ cu operația de înmulțire este subgrup al grupului multiplicativ $\mathbb{Q}^*$ al numerelor raționale nenule, care la rîndul său este subgrup al lui $\mathbb{R}^*$.

De asemenea, cu notațiile din exemplele precedente, G' este un subgrup al lui U, iar ambele sînt subgrupuri ale grupului multiplicativ $\mathbb{C}^*$ al numerelor complexe nenule.

În cele ce urmează sînt determinate toate subgrupurile grupului aditiv $\mathbb{Z}$ al numerelor întregi.

Propoziția 2.2. *Pentru $n \in \mathbb{Z}$, $n \geqslant 0$, mulțimea $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ este un subgrup al grupului aditiv $\mathbb{Z}$. Reciproc, dacă H este un subgrup al grupului aditiv $\mathbb{Z}$, atunci există $n \in \mathbb{Z}$, $n \geqslant 0$, astfel încît $H = n\mathbb{Z}$.*

Demonstrație. Dacă $x, y \in n\mathbb{Z}$, $x = nh$ și $y = nk$ cu $h, k \in \mathbb{Z}$, atunci

$$x - y = n(h - k) \in n\mathbb{Z}$$

și, conform variantei aditive a propoziției precedente, rezultă că $n\mathbb{Z}$ este subgrup al lui $\mathbb{Z}$.

Reciproc, fie H un subgrup oarecare al grupului aditiv $\mathbb{Z}$. Dacă $H = \{0\}$, adică H este subgrupul nul, atunci $H = n\mathbb{Z}$ cu $n = 0$. Dacă $H \neq \{0\}$, există $x \in H$, $x \neq 0$. Datorită lui 2°; și $-x \in H$.

Rezultă că H conține numere întregi pozitive. Fie n cel mai mic număr întreg pozitiv din H. Avem

$$0 \in H,\ n \in H,\ 2n = n + n \in H,\ 3n = 2n + n \in H, \ldots$$

și

$$-n \in H,\ -2n \in H,\ -3n \in H, \ldots$$

după cum rezultă aplicînd 1° și 2°. Deci $n\mathbb{Z} \subset H$. Fie $x \in H$. Conform teoremei împărțirii cu rest la numere întregi, se poate scrie

$$x = nq + r, \text{ cu } 0 \leqslant r < n.$$

Deoarece x și nq sînt din H, rezultă $r = x - nq \in H$. Dar $0 \leqslant \leqslant r < n$ și n este cel mai mic întreg strict pozitiv din H; rezultă că $r = 0$, deci $x = nq \in n\mathbb{Z}$. Așadar, $H \subset n\mathbb{Z}$, de unde $H = n\mathbb{Z}$.

Dacă G și G' sînt două grupuri, de exemplu multiplicative, o aplicație $\varphi : G \to G'$ se numește *omomorfism de* grupuri dacă

$$\varphi(xy) = \varphi(x)\,\varphi(y), \text{ oricare ar fi } x, y \in G.$$

Propoziția 2.3. *Dacă G și G' sînt două grupuri, e și e' elementele neutre ale lui G, respectiv G' și $\varphi : G \to G'$ un omomorfism de grupuri, atunci :*

1) $\varphi(e) = e'$;

2) *pentru orice $x \in G$ avem* $\varphi(x^{-1}) = (\varphi(x))^{-1}$.

Demonstrație. 1) Avem

$$\varphi(e) = \varphi(ee) = \varphi(e)\,\varphi(e),$$

de unde, înmulțind la stînga cu $(\varphi(e))^{-1}$, rezultă

$$e' = \varphi(e).$$

2) Avem $e' = \varphi(e) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$ și analog, $e' = \varphi(x^{-1})\,\varphi(x)$. Deci

$$\varphi(x^{-1}) = (\varphi(x))^{-1}.$$

Un omomorfism $\varphi : G \to G'$ se numește *izomorfism* dacă există un omomorfism $\psi : G' \to G$ astfel încît

$$\varphi \circ \psi = 1_{G'} \text{ și } \psi \circ \varphi = 1_G.$$

Scriem atunci $\varphi : G \xrightarrow{\sim} G'$.

Un omomorfism de grupuri definit pe grupul G și cu valori tot în G se numește *endomorfism* al lui G.

Un endomorfism al lui G care este şi izomorfism se numeşte *automorfism* al lui G.

Exemple. 1. Funcţia $\theta : G \to G'$, astfel încît $\theta(x) = e'$, oricare ar fi $x \in G$, este un omomorfism, numit *omomorfismul nul.*

2. Funcţia $\varphi : \mathbb{Z} \to \{1, -1\}$ definită prin

$$\varphi(x) = \begin{cases} 1, & \text{dacă } x \text{ este par,} \\ -1, & \text{dacă } x \text{ este impar,} \end{cases}$$

este un omomorfism de la grupul aditiv al numerelor întregi la grupul multiplicativ $\{1, -1\}$. Verificarea este imediată.

3. $\psi : \mathbb{Z} \to \mathbb{Z}$ definită prin $\psi(x) = 3x$ este un endomorfism al grupului aditiv $\mathbb{Z}$.

Fie $\varphi : G \to G'$ un omomorfism de grupuri. Dacă φ este o funcţie injectivă (surjectivă), omomorfismul φ se numeşte *injectiv* (*surjectiv*). Dacă φ este bijectivă, φ se numeşte *omomorfism bijectiv.*

Propoziţia 2.4. *Un omomorfism de grupuri* $\varphi : G \to G'$ *este un izomorfism dacă şi numai dacă este un omomorfism bijectiv.*

Demonstraţie. Avînd în vedere propoziţia 1.3, rezultă că este suficient să demonstrăm că dacă φ este omomorfism bijectiv iar $\psi : G' \to G$ este inversa funcţiei φ, atunci ψ este omomorfism. Aşadar, va trebui arătat că, oricare ar fi $y, y' \in G'$, avem

$$\psi(yy') = \psi(y)\, \psi(y').$$

Cum φ este injectivă, este suficient să demonstrăm că

$$\varphi(\psi(yy')) = \varphi(\psi(y)\, \psi(y')).$$

Într-adevăr,

$$\varphi(\psi(y)\psi(y')) = \varphi(\psi(y))\, \varphi(\psi(y')) = yy' = \varphi(\psi(yy')).$$

Exemplu. Dacă $\mathbb{R}_+^*$ este grupul multiplicativ al numerelor reale strict pozitive şi $\mathbb{R}$ grupul aditiv al numerelor reale, funcţia

$$\ln : \mathbb{R}_+^* \to \mathbb{R}$$

este un izomorfism, omomorfismul invers fiind dat de aplicaţia $x \to e^x$ de la $\mathbb{R}$ la $\mathbb{R}_+^*$.

Dăm acum o caracterizare a omomorfismelor injective de grupuri. Dacă $\varphi : G \to G'$ este un omomorfism, definim

$$\text{Ker } \varphi = \{x \in G \mid \varphi(x) = e'\}.$$

Dacă $x, y \in \text{Ker } \varphi$, adică $\varphi(x) = \varphi(y) = e'$, atunci

$$\varphi(xy^{-1}) = \varphi(x)\, \varphi(y^{-1}) = \varphi(x)\, (\varphi(y))^{-1} = e'e' = e', \text{ deci } xy^{-1} \in \text{Ker } \varphi.$$

Așadar, Ker φ este un subgrup al lui G care se numește *nucleul* omomorfismului φ. De asemenea, Im $\varphi = \varphi(G)$ se vede imediat că este un subgrup al lui G', numit *imaginea* omomorfismului φ.

Propoziția 2.5. *Fie* $\varphi : G \to G'$ *un omomorfism de grupuri. Atunci* φ *este omomorfism injectiv dacă și numai dacă* Ker $\varphi = \{e\}$.

Demonstrație. Fie φ injectiv și să arătăm că Ker $\varphi = \{e\}$. După propoziția 2.3, $\varphi(e) = e'$. Să presupunem că $x \in \text{Ker } \varphi$, adică $\varphi(x) = e' = \varphi(e)$. Cum φ este injectivă, rezultă $x = e$. Reciproc, fie $\varphi(x) = \varphi(y)$. Atunci $\varphi(x)\,(\varphi(y))^{-1} = e'$, adică $\varphi(x)\,\varphi(y^{-1}) = e'$ sau $\varphi(xy^{-1}) = e'$ și deci $xy^{-1} = e$. Așadar $x = y$ și deci φ este injectivă.

§ 3. Relații de echivalență

Fie M o mulțime nevidă. Se spune că pe M este definită o *relație binară*, dacă s-a dat o submulțime R a produsului cartezian $M \times M$. Elementele $x, y \in M$ sînt în relația R și scriem xRy dacă $(x, y) \in R$.

Definiția 3.1. O relație binară R pe M se numește *relație de echivalență* dacă are proprietățile :

1° pentru orice $x \in M$, xRx (*reflexivitate*) ;

2° dacă $x, y \in M$ și xRy, atunci yRx (*simetrie*) ;

3° dacă $x, y, z \in M$, din xRy și yRz rezultă xRz (*tranzitivitate*).

Relațiile de echivalență se vor nota în continuare în mai multe moduri. Dacă R este o relație de echivalență pe mulțimea M, să notăm, pentru orice $x \in M$, cu $\hat{x}$ submulțimea

$$\hat{x} = \{y \mid y \in M, yRx\}.$$

Această submulțime se numește *clasa de echivalență a elementului* x.

Propoziția 3.1. *Fie M o mulțime și R o relație de echivalență pe M. Atunci clasele de echivalență determinate de R pe M au proprietățile :*

1° $\hat{x} \neq \emptyset$, *oricare ar fi* $x \in M$ (*orice clasă de echivalență este nevidă*).

2° *Dacă* xRy, *atunci* $\hat{x} = \hat{y}$, *iar în caz contrar*, $\hat{x} \cap \hat{y} = \emptyset$.

3° $M = \bigcup_{x \in M} \hat{x}$.

Demonstrație. 1° Deoarece xRx, rezultă $x \in \hat{x}$, deci $\hat{x} \neq \emptyset$.

2° Dacă xRy și $z \in \hat{x}$, atunci zRx. Din tranzitivitatea relației R rezultă zRy, adică $z \in \hat{y}$. Astfel $\hat{x} \subset \hat{y}$ și analog rezultă $\hat{y} \subset \hat{x}$, deci $\hat{x} = \hat{y}$.

Să presupunem că $z \in \hat{x} \cap \hat{y}$; atunci zRx și zRy și deci xRy.

3° Dacă $y \in M$, atunci $y \in \hat{y}$ și deci $y \in \bigcup_{z \in M} \hat{z}$.

Dacă R este o relație de echivalență pe mulțimea M, se notează cu M/R mulțimea avînd ca elemente clasele de echivalență $\hat{x}$, unde x parcurge pe M. Mulțimea M/R este numită *mulțimea cît* (*factor*) a lui M în raport cu relația de echivalență R. Se spune că mulțimea $\{x_i\}_{i \in I}$ de elemente din M formează un *sistem complet de reprezentanți* pentru relația R, dacă :

1° dacă $i \neq j$, atunci x_i nu este în relația R cu x_j,

2° oricare ar fi $x \in M$, există $i \in I$ astfel încît xRx_i.

Cu alte cuvinte, $\{x_i\}_{i \in I}$ este un sistem complet de reprezentanți dacă $\hat{x}_i \neq \hat{x}_j$ pentru $i \neq j$ și oricare $\hat{x} \in M/R$, există x_i, astfel încît $\hat{x} = \hat{x}_i$.

Dacă se asociază fiecărui element $x \in M$ clasa sa de echivalență $\hat{x}$ în raport cu R, se obține o aplicație surjectivă :

$$p : M \to M/R$$

numită *surjecția canonică* a lui M pe M/R.

Exemplu. Fie $n > 0$ un număr întreg. Pe mulțimea $\mathbb{Z}$ a numerelor întregi se definește următoarea relație binară : dacă $x, y \in \mathbb{Z}$, atunci $x \equiv y (\text{mod } n)$ dacă și numai dacă n divide pe $x - y$.

Această relație binară care este, evident, o relație de echivalență este numită *relația de congruență modulo n*. Ne propunem să descriem mulțimea factor a lui $\mathbb{Z}$ în raport cu această relație de echivalență.

Pentru $n = 1$, cum toate numerele întregi sînt congruente între ele modulo 1, rezultă că în acest caz mulțimea cît are un singur element.

Fie $n > 1$ și fie $x \in \mathbb{Z}$. După teorema împărțirii cu rest pentru numerele întregi $x = qn + r$ cu $0 \leqslant r \leqslant n - 1$. De aici rezultă $x \equiv r (\text{mod } n)$. Așadar, orice

$x \in \mathbb{Z}$ aparţine clasei de echivalenţă determinate de un număr r cu $0 \leqslant r \leqslant n-1$ Mai mult, dacă $0 \leqslant r, s \leqslant n-1$ şi $r \equiv s (\mathrm{mod}\, n)$, atunci $n | r-s$, adică $r-s=0$ şi deci $r=s$. Aşadar numerele $0, 1, 2, \ldots, n-1$ constituie un sistem complet de reprezentanţi pentru congruenţa modulo n. Deci

$$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\},$$

unde prin $\hat{x}$ s-a notat clasa de echivalenţă a numărului x.

§ 4. Relaţii de echivalenţă pe grupuri

Fie G un grup şi H un subgrup al său. Considerăm pe G următoarele relaţii binare :

Dacă $x, y \in G$, atunci

$$xR^s y \text{ dacă şi numai dacă } x^{-1}y \in H$$

şi

$$xR^d y \text{ dacă şi numai dacă } xy^{-1} \in H$$

Aceste relaţii binare sînt relaţii de echivalenţă.

Să demonstrăm, de exemplu, că prima relaţie este o relaţie de echivalenţă. Dacă $x \in G$, atunci din $x^{-1}x = e \in H$ rezultă că $xR^s x$ (reflexivitatea). Dacă $xR^s y$, atunci $x^{-1}y \in H$ şi deci $y^{-1}x = (x^{-1}y)^{-1} \in H$, de unde $yR^s x$ (simetria). În sfîrşit, dacă $xR^s y$ şi $yR^s z$, atunci $x^{-1}y \in H$ şi $y^{-1}z \in H$. Deci $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$, adică $xR^s z$ (tranzitivitatea).

Analog, se demonstrează că R^d este relaţie de echivalenţă.

Relaţiile de echivalenţă de mai sus se numesc *relaţii de congruenţă la stînga*, respectiv *la dreapta în raport cu H* sau *modulo H*.

Să notăm cu $\hat{x}$, respectiv $\hat{\hat{x}}$, clasa de echivalenţă a elementului $x \in G$ în raport cu R^s, respectiv R^d şi o vom numi *clasa de echivalenţă la stînga*, respectiv *clasa de echivalenţă la dreapta a lui x modulo H*. Fie G/R^s şi G/R^d *mulţimile* factor corespunzătoare lui R^s şi R^d.

Lema 4.1. *Fie G un grup şi H un subgrup al său. Dacă $x \in G$ este un element oarecare, atunci :*

$$\hat{x} = \{xh \mid h \in H\} \qquad \text{(notată cu } xH)$$
$$\hat{\hat{x}} = \{hx \mid h \in H\} \qquad \text{(notată cu } Hx)$$

Demonstrație. Din definiție avem

$$\hat{x} = \{y \in G \mid xR^s y\} = \{y \in G \mid x^{-1} y \in H\} =$$

$$= \{y \in G \mid \text{există } h \in H, x^{-1} y = h\} = \{y \in G \mid y = xh\} = xH$$

La fel se arată că $\hat{\hat{x}} = Hx$.

Propoziția 4.2. *Dacă G este un grup și H un subgrup al său, fie R^s și R^d relațiile de congruență modulo H. Atunci aplicația*

$$\varphi : G/R^s \to G/R^d$$

dată de $\varphi(xH) = Hx^{-1}$ este bijectivă.

Demonstrație. Să arătăm mai întîi că φ este bine definită. Într-adevăr, dacă $xH = yH$, adică $xR^s y$, atunci $x^{-1}y \in H$ sau $x^{-1}(y^{-1})^{-1} \in H$. Deci $x^{-1}R^d y^{-1}$, adică $Hx^{-1} = Hy^{-1}$, ceea ce înseamnă că φ este bine definită. Dacă acum $\varphi(xH) = \varphi(yH)$, atunci $Hx^{-1} = Hy^{-1}$, de unde rezultă imediat că $xH = yH$, deci φ este injectivă. Faptul că φ este surjectivă este clar deoarece $\varphi(x^{-1}H) = H(x^{-1})^{-1} = Hx$.

În particular, dacă una dintre mulțimile G/R^s sau G/R^d este finită, atunci și cealaltă este finită și ele au același număr de elemente. Se spune în acest caz că H are indice finit în G sau că H este un subgrup de indice finit al lui G, iar numărul de elemente ale mulțimilor G/R^s sau G/R^d (care este același) se numește *indicele* lui H în G și se notează $[G : H]$.

Se spune că un grup G este *finit* dacă mulțimea elementelor sale este finită, iar numărul de elemente ale lui G se numește *ordinul* său și se notează ord G.

Evident, dacă G are ordin finit, atunci orice subgrup al său are ordin finit și mai mult, indicele oricărui subgrup este finit.

Teorema 4.3 (*Lagrange*). *Dacă G este un grup finit și H un subgrup al său, atunci*

$$\text{ord}\, G = [G : H] \cdot \text{ord}\, H$$

Demonstrație. Conform propoziției precedente, putem să facem demonstrația, considerînd, de exemplu, numai relația de echivalență R^s pe G.

Fie x_1H, x_2H, ..., x_kH clasele de echivalență la stînga modulo H. Așadar $k = [G : H]$. Vom arăta mai întîi că orice două clase de mai sus au același număr de elemente. Pentru aceasta arătăm că aplicația $\psi : x_iH \to x_jH$ definită prin $\psi(x_ih) = x_jh$ este bijectivă. Într-adevăr, dacă $\psi(x_ih) = \psi(x_ih')$, rezultă $x_jh = x_jh'$, de unde $h = h'$ și astfel $x_ih = x_i h'$. Deci ψ este injectivă. Mai mult, evident, din definiție rezultă că ψ este surjectivă. Cum H este o clasă de echivalență și anume clasa elementului neutru, rezultă că numărul de elemente ale oricărei clase coincide cu ordinul lui H. Dar

$$G = \bigcup_{i=1}^{k} x_iH \text{ și } x_iH \cap x_jH = \emptyset, \text{ pentru } i \neq j,$$

de unde

$$\text{card } G = \sum_{i=1}^{k} \text{card } (x_iH) = k \text{ ord } H.$$

Deci $\text{ord } G = [G : H] \cdot \text{ord } H$.

§ 5. Subgrup normal. Grup factor

Definiția 5.1. Fie G un grup și H un subgrup al său. Se spune că H este *subgrup normal* sau *divizor normal* al lui G dacă pentru orice $x \in G$ și $h \in H$ avem $xhx^{-1} \in H$.

Iată alte caracterizări ale subgrupului normal:

Propoziția 5.2. *Fie H un subgrup al grupului G. Atunci următoarele afirmații sînt echivalente*:

1) *H este subgrup normal al lui G.*
2) *Pentru orice $x \in G$ avem $xH = Hx$.*
3) *Pentru orice $x \in G$ avem $xHx^{-1} = H$.*

Demonstrație. 1) $\Rightarrow$ 2). Dacă $y \in xH$, atunci $y = xh$ cu $h \in H$. Deci $yx^{-1} = xhx^{-1} \in H$, adică $y \in Hx$. Deci $xH \subset Hx$. Analog rezultă $Hx \subset xH$, deci egalitate. 2) $\Rightarrow$ 3) și 3) $\Rightarrow$ 1) sînt evidente.

În particular, dacă G este grup abelian, atunci, evident, toate subgrupurile sale sînt normale.

Din propoziția precedentă este clar că, dacă H este un subgrup normal al lui G, atunci relațiile de congruență R^s și R^d

în raport cu H coincid. În acest caz se spune, pe scurt, ***congruența*** ***R modulo H***. Cele două mulțimi factor G/R^s și G/R^d de asemenea coincid, mulțimea factor G/R fiind notată cu G/H.

Propoziția 5.3. *Dacă G este un grup și H un subgrup normal al său, atunci pe mulțimea factor G/H se poate defini o operație algebrică împreună cu care G/H devine grup.*

Demonstrație. Dacă $\hat{x}, \hat{y} \in G/H$, definim

$$\hat{x}\hat{y} = \widehat{xy}.$$

Să arătăm, mai întîi, că această operație este bine **definită**, adică nu depinde de alegerea reprezentanților. **Într-adevăr**, fie $\hat{x} = \hat{x}'$ și $\hat{y} = \hat{y}'$. Atunci $x^{-1}x' \in H$ și $y^{-1}y' \in H$, adică există $h_1, h_2 \in H$ astfel încît $x' = xh_1$ și $y' = yh_2$. Deci $x'y' = xh_1yh_2$. Dar, cum H este subgrup normal, există $h_3 \in H$ astfel încît $h_1y = yh_3$, de unde se obține $x'y' = xyh_3h_2$ iar $h_3h_2 \in H$. Deci $(xy)^{-1}(x'y') = h_3h_2 \in H$, adică

$$\widehat{xy} = \widehat{x'y'}.$$

Operația este asociativă, deoarece dacă $\hat{x}, \hat{y}, \hat{z} \in G/H$, atunci

$$\hat{x}(\hat{y}\hat{z}) = \hat{x}\widehat{yz} = \widehat{x(yz)} = \widehat{(xy)z} = \widehat{xy}\hat{z} = (\hat{x}\hat{y})\hat{z}.$$

Operația admite element neutru $\hat{e} \in G/H$, deoarece pentru oricare $\hat{x} \in G/H$ avem evident

$$\hat{x}\hat{e} = \hat{e}\hat{x} = \hat{x}.$$

De asemenea, orice element $\hat{x} \in G/H$ are un invers care este $\widehat{x^{-1}} \in G/H$, deoarece

$$\hat{x}\widehat{x^{-1}} = \widehat{xx^{-1}} = \hat{e} \text{ și } \widehat{x^{-1}}\hat{x} = \widehat{x^{-1}x} = \hat{e}.$$

Deci G/H este un grup.

Definiția 5.2. Grupul G/H construit la propoziția precedentă se numește *grupul factor* (*cît*) al lui G în raport cu subgrupul normal H.

Aplicaţia canonică (vezi §3)

$$p : G \to G/H,\ p(x) = \hat{x}$$

este un omomorfism de grupuri. Într-adevăr, dacă $\hat{x}, \hat{y} \in G/H$, atunci

$$p(xy) = \widehat{xy} = \hat{x}\hat{y} = p(x)\,p(y).$$

Exemplu. Fie $H \subset \mathbb{Z}$ un subgrup nenul al grupului aditiv $\mathbb{Z}$. Atunci $H = n\mathbb{Z}$ pentru un anumit număr $n > 0$.

Să vedem cine este grupul factor $\mathbb{Z}/n\mathbb{Z}$. Două numere $x, y \in \mathbb{Z}$, xRy (mod $n\mathbb{Z}$) dacă $x - y \in n\mathbb{Z}$, adică $n \mid x - y$. Deci xRy (mod $n\mathbb{Z}$) dacă şi numai dacă $x \equiv y$ (mod n). Atunci

$$\mathbb{Z}/n\mathbb{Z} = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\}.$$

Operaţia de grup pe $\mathbb{Z}/n\mathbb{Z}$ este

$$\hat{x} + \hat{y} = \widehat{x+y}, \text{ oricare ar fi } \hat{x}, \hat{y} \in \mathbb{Z}/n\mathbb{Z}.$$

Deci grupul factor al lui $\mathbb{Z}$ în raport cu $n\mathbb{Z}$ este $(\mathbb{Z}_n, +)$.

Fie G şi G' două grupuri şi $\varphi : G \to G'$ un omomorfism de grupuri. Am notat prin

$$\text{Ker } \varphi = \{x \in G \mid \varphi(x) = e'\}$$

şi am demonstrat (vezi §2) că acesta este un subgrup al lui G. Vom demonstra că Ker φ este subgrup normal. Într-adevăr, dacă $x \in G$ şi $y \in \text{Ker } \varphi$, atunci $xyx^{-1} \in \text{Ker } \varphi$, deoarece $\varphi(xyx^{-1}) = \varphi(x)\,\varphi(y)\,\varphi(x^{-1}) = \varphi(x)\,e'(\varphi(x))^{-1} = e'$. Aşadar, se poate vorbi de grupul factor $G/\text{Ker } \varphi$. Fie $p : G \to G/\text{Ker } \varphi$ omomorfismul natural de la grupul G la grupul factor $G/\text{Ker } \varphi$. De asemenea, am arătat că Im φ este un subgrup al lui G'. Mai mult, avem :

Teorema 5.4 (*fundamentală de izomorfism*). *Fie $\varphi : G \to G'$ un omomorfism de grupuri. Atunci există un izomorfism canonic*

$$\bar{\varphi} : G/\text{ Ker } \varphi \xrightarrow{\sim} \text{Im } \varphi.$$

Demonstrație. Definim $\overline{\varphi}$ prin $\overline{\varphi}(\hat{x}) = \varphi(x)$. Aplicația $\overline{\varphi}$ este bine definită, deoarece din $\hat{x} = \hat{y}$ rezultă $x^{-1}y \in \operatorname{Ker} \varphi$, adică $\varphi(x^{-1}y) = e'$. Dar $\varphi(x^{-1}y) = \varphi(x^{-1})\varphi(y) = (\varphi(x))^{-1}\varphi(y)$, de unde $(\varphi(x))^{-1}\varphi(y) = e'$, adică $\varphi(x) = \varphi(y)$. Așadar, $\overline{\varphi}(\hat{x}) = \overline{\varphi}(\hat{y})$. Faptul că $\overline{\varphi}$ este surjectivă este evident, deoarece orice element din Im φ se scrie $\varphi(x)$ cu $x \in G$. Fie $\overline{\varphi}(\hat{x}) = \overline{\varphi}(\hat{y})$. Atunci $\varphi(x) = \varphi(y)$ și deci $\varphi(x^{-1}y) = e'$ și astfel $x^{-1}y \in \operatorname{Ker} \varphi$, ceea ce înseamnă că $\hat{x} = \hat{y}$. Deci $\overline{\varphi}$ este injectivă. Ținînd seama de faptul că φ este omomorfism de grupuri, rezultă

$$\overline{\varphi}(\hat{x}\hat{y}) = \overline{\varphi}(\widehat{xy}) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}(\hat{x})\overline{\varphi}(\hat{y}),$$

adică φ este un omomorfism de grupuri. Deci $\overline{\varphi}$ este un izomorfism.

§ 6. Grupuri ciclice

Fie G un grup multiplicativ și $a \in G$ un element al său. Pentru orice $n \in \mathbb{Z}$ definim

$$a^n = \begin{cases} \underbrace{a \ a \ \ldots a}_{n \text{ factori}}, & \text{dacă } n > 0, \\ e, & \text{dacă } n = 0, \\ \underbrace{a^{-1}a^{-1} \ldots a^{-1}}_{n \text{ factori}}, & \text{dacă } n < 0. \end{cases}$$

Dacă $n \in \mathbb{Z}$, atunci

$$a^n a^{-n} = a^{-n} a^n = e$$

și deci a^{-n} este inversul lui a^n, adică $a^{-n} = (a^n)^{-1}$.

Dacă $m, n \in \mathbb{Z}$ sînt două numere întregi oarecare, atunci

$$a^m a^n = a^{m+n} \text{ și } (a^m)^n = a^{mn}.$$

Verificarea acestor relații, care se face ușor prin inducție, o lăsăm pe seama cititorului.

Dacă grupul G este aditiv, atunci definim

$$na = \begin{cases} \underbrace{a + a + \ldots + a}_{n \text{ termeni}} & , \text{ dacă } n > 0, \\ 0 & , \text{ dacă } n = 0, \\ \underbrace{(-a) + (-a) + \ldots + (-a)}_{n \text{ termeni}}, & \text{dacă } n < 0. \end{cases}$$

Avem

$$ma + na = (m + n)a \text{ și } m(na) = (mn)a,$$

oricare ar fi $m, n \in \mathbb{Z}$.

G fiind un grup (în notație multiplicativă) și $a \in G$ un element oarecare, să notăm cu

$$\langle a \rangle = \{a^k | k \in \mathbb{Z}\}$$

Este clar că $\langle a \rangle$ este subgrup al lui G, numit *subgrupul ciclic generat de a.*

Definiția 6.1. Un grup G se numește *ciclic* dacă există $a \in G$, astfel încît $G = \langle a \rangle$ (adică toate elementele sale sînt puteri ale unui anumit element $a \in G$). Elementul a se numește *generator* al grupului ciclic G.

Grupul aditiv $\mathbb{Z}$ este ciclic, de generator 1, și fiecare grup aditiv $\mathbb{Z}_n$ este ciclic, cu generatorul clasa lui 1 modulo n. Vom demonstra mai jos că orice grup ciclic este izomorf cu $\mathbb{Z}$ sau cu $\mathbb{Z}_n$.

Fie G un grup multiplicativ și $a \in G$ un element al său. Să considerăm aplicația $\eta : \mathbb{Z} \to G$ definită astfel :

$$\eta(n) = a^n, \; n \in \mathbb{Z}.$$

Imaginea aplicației η este, evident, subgrupul ciclic generat de a. Ne punem problema cînd două puteri ale lui a sînt egale.

Definiția 6.2. Se spune că un element a al grupului G este de *ordin infinit* în G dacă toate puterile sale sînt distincte. În caz contrar, adică dacă există $i, j \in \mathbb{Z}$, $i \neq j$, astfel încît $a^i = a^j$, se spune că a este de *ordin finit.*

Observație. Elementul $a \in G$ este de ordin infinit dacă aplicația η definită mai sus este injectivă și este de ordin finit cînd η nu este injectivă.

Fie $a \in G$ un element de ordin finit și $i < j$ astfel încît $a^i = a^j$. Atunci $a^{j-i} = e$ și, prin urmare, există o putere pozitivă a lui a egală cu elementul neutru. Cel mai mic număr întreg pozitiv n astfel că $a^n = e$ se numește *ordinul elementului* a și se notează cu ord a:

$$\text{ord } a = \min \{k \mid a^k = e, \ k > 0\}.$$

Astfel, fiecare element al unui grup are ca ordin un număr întreg pozitiv sau infinit.

Observăm că elementul neutru al lui G este singurul element de ordin 1 al grupului.

Propoziția 6.1. *Dacă* $a \in G$ *este un element de ordin* n, *atunci subgrupul ciclic generat de* a *are exact* n *elemente și anume*

$$\langle a \rangle = \{e, \ a, \ a^2, \ \ldots, a^{n-1}\}.$$

Demonstrație. Dacă $n = \text{ord } a$, pentru orice a^k punem, după teorema împărțirii cu rest, $k = nq + r$ cu $0 \leqslant r < n$. Deci $a^k = a^{nq+r} = (a^n)^q \cdot a^r$. Așadar, subgrupul generat de a este $\{e, a, a^2, \ldots, a^{n-1}\}$. Aceste elemente sînt toate distincte. Într-adevăr, dacă am avea $a^i = a^j$, $0 \leqslant i < j \leqslant n - 1$, atunci $a^{j-i} = e$ și $0 < j - i < n$, deci rezultă contradicție.

Din teorema lui Lagrange și propoziția precedentă rezultă

Corolarul 6.2. *Dacă* G *este un grup finit, atunci ordinul oricărui element al său (care evident este finit) divide ordinul lui* G.

Am observat că grupurile aditive $\mathbb{Z}$ și $\mathbb{Z}_n$ $(n>0)$ sînt ciclice. Următoarea teoremă arată că acestea sînt singurele tipuri de grupuri ciclice.

Teorema 6.3. *Un grup ciclic* G *este izomorf fie cu grupul* $\mathbb{Z}$ *al numerelor întregi, fie cu un anume grup* $\mathbb{Z}_n$ $(n > 0)$ *de clase de resturi modulo* n.

Demonstrație. Fie $G = \langle a \rangle$ și aplicația $\eta : \mathbb{Z} \to G$, definită prin $\eta(n) = a^n$. Avem

$$\eta(m + n) = a^{m+n} = a^m a^n = \eta(m) \, \eta(n)$$

şi deci η este un omomorfism de grupuri. Acest omomorfism este surjectiv, deci Im $\eta = G$. Dacă calculăm nucleul lui η, Ker η, pot fi două cazuri : 1) Ker $\eta = \{0\}$, 2) Ker $\eta \neq \{0\}$. În primul caz, conform teoremei de izomorfism, avem

$$\mathbb{Z}/\{0\} \xrightarrow{\sim} \text{Im } \eta, \text{ adică } \mathbb{Z} \xrightarrow{\sim} G.$$

În cazul al doilea, Ker η este de forma $n\mathbb{Z}$ cu $n \in \mathbb{Z}$, $n > 0$. În acest caz, conform teoremei de izomorfism, avem

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \text{Im } \eta, \text{ adică } \mathbb{Z}_n \xrightarrow{\sim} G.$$

Din izomorfismul $\mathbb{Z}_n \xrightarrow{\sim} G$ dat de $\hat{r} \to a^r$ avem că $a^{kn} = e$, oricare ar fi $k \in \mathbb{Z}$ şi dacă $a^l = e$, atunci $n \mid l$. Mai general, $a^r = a^s$ dacă şi numai dacă $r \equiv s \pmod{n}$.

Observaţie. Cele de mai sus pot fi reformulate astfel. Fie G un grup ciclic şi a un generator al său. 1. Dacă a este de ordin infinit, atunci G este izomorf cu grupul $\mathbb{Z}$. 2. Dacă a este de ordin n (finit), atunci G este izomorf cu grupul $\mathbb{Z}_n$.

Propoziţie 6.4. *Orice subgrup şi orice grup factor al unui grup ciclic este ciclic.*

Demonstraţie. Dacă $G = \langle a \rangle$ este ciclic iar H un subgrup al său, atunci G/H este ciclic generat de clasa lui a modulo H. Să arătăm că orice subgrup al unui grup ciclic este ciclic. Într-adevăr, în privinţa lui $\mathbb{Z}$ am arătat că subgrupurile sale sînt de tipul $n\mathbb{Z}$ (vezi propoziţia 2.2), sînt deci ciclice. Fie G un grup ciclic finit al cărui generator a este de ordin n şi H un subgrup al său. Considerăm cel mai mic întreg pozitiv k astfel încît $a^k \in H$. Atunci, după teorema împărţirii cu rest, $n = kq + r$ cu $0 \leqslant r < k$. Deoarece $e = a^n \in H$ şi $a^{-kq} = (a^{kq})^{-1} \in H$, din $e = a^n = a^{kq+r} = a^{kq} \cdot a^r$ rezultă $a^r \in H$. Cum k este cel mai mic întreg pozitiv încît $a^k \in H$, rezultă $r = 0$. Deci $n = kq$ şi

$$H = \{e, a^k, a^{2k}, \ldots, a^{(q-1)k}\},$$

adică H este ciclic generat de a^k.

Generatorii unui grup ciclic finit se caracterizează astfel :

Propoziţia 6.5. *Un element $\hat{x} \in \mathbb{Z}_n$ este generator al grupului aditiv $\mathbb{Z}_n$ dacă şi numai dacă x este prim cu n.*

Demonstrație. Dacă $\hat{x}$ este un generator al lui $\mathbb{Z}_n$, atunci există $a \in \mathbb{Z}$ astfel încît $\hat{1} = a\hat{x}$. Dar $a\hat{x} = \widehat{ax} = \hat{1}$ și deci $ax \equiv 1 \pmod{n}$. Așadar $n \mid ax - 1$ și deci există $b \in \mathbb{Z}$ astfel încît $ax - 1 = bn$ sau $ax - bn = 1$. Astfel x este prim cu n. Reciproc, dacă x este prim cu n, atunci există a, $b \in \mathbb{Z}$, astfel încît $ax + bn = 1$. Trecînd relația în $\mathbb{Z}_n$, se obține $\widehat{ax + bn} = \hat{1}$ sau $\widehat{ax} + \widehat{bn} = \hat{1}$ și deci $\hat{a}\hat{x} = \hat{1}$. Dacă $\hat{y} \in \mathbb{Z}_n$ este un element oarecare, atunci $\hat{y} = y\hat{1} = (ya)\hat{x}$. Astfel $\hat{x}$ generează grupul $\mathbb{Z}_n$.

În cap. I, § 3, am arătat că grupul U_n al rădăcinilor de ordin n ale unității este ciclic, un generator al său fiind $z_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. O rădăcină $z_k = \frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ care generează grupul U_n se numește *primitivă*. Conform celor de mai sus, rezultă că z_k este rădăcină primitivă dacă și numai dacă k este prim cu n.

§ 7. Grupuri de permutări

Fie M o mulțime. Am observat (vezi § 2, exemplul 6), că mulțimea $\sigma(M)$ a aplicațiilor bijective ale lui M în M formează față de compunere un grup, care se numește *grupul permutărilor mulțimii M*.

Propoziția 7.1. *Dacă M și M' sînt două mulțimi între care există o aplicație bijectivă, atunci grupurile de permutări $\sigma(M)$ și $\sigma(M')$ sînt izomorfe.*

Demonstrație. Fie $u : M \to M'$ o aplicație bijectivă. Cum compunerea de aplicații bijective este bijectivă, atunci $u \circ f \circ u^{-1} \in \sigma(M')$ și se definește

$$\varphi : \sigma(M) \to \sigma(M') \text{ prin } \varphi(f) = u \circ f \circ u^{-1}.$$

Demonstrăm că φ este un izomorfism. Într-adevăr, $\varphi(f \circ g) = u \circ (f \circ g) \circ u^{-1} = u \circ f \circ (u^{-1} \circ u) \circ g \circ u^{-1} = (u \circ f \circ u^{-1}) \circ (u \circ g \circ u^{-1}) = \varphi(f) \circ \varphi(g)$ și deci φ este omomorfism.

Dacă $\varphi(f) = \varphi(f')$, atunci $u \circ f \circ u^{-1} = u \circ f' \circ u^{-1}$, de unde $f = f'$, deci φ este injectivă. Mai mult, dacă $h \in \sigma(M')$, atunci $\varphi(u^{-1} \circ h \circ u) = u \circ (u^{-1} \circ h \circ u) \circ u^{-1} = h$ şi deci φ este şi surjectivă.

În particular, dacă M este o mulţime cu n elemente, atunci există o bijecţie între M şi $\{1, 2, \ldots, n\}$ şi pentru a studia grupul permutărilor unei mulţimi cu n elemente este suficient să studiem grupul permutărilor mulţimii $\{1, 2, \ldots, n\}$. Grupul de permutări al mulţimii $\{1, 2, \ldots, n\}$ se numeşte şi ***grupul simetric de grad n***, şi-l vom nota cu σ_n. Un element din σ_n se numeşte *permutare* de n elemente. Elementul neutru din σ_n se numeşte *permutarea identică*.

Fie $\sigma \in \sigma_n$ o permutare de n elemente. De obicei, pentru permutarea σ (care este o funcţie bijectivă de la $\{1, 2, \ldots, n\}$ la $\{1, 2, \ldots, n\}$) se foloseşte notaţia

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Numerele $\sigma(1), \sigma(2), \ldots, \sigma(n)$ sînt tot numerele $1, 2, \ldots, n$, eventual în altă ordine. Este bine ştiut că ord $\sigma_n = n!$.

Fie $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$ o permutare de n elemente, unde $\sigma(i) = a_i$. Un cuplu (a_i, a_j) se numeşte *inversiune* dacă $i < j$ şi $a_i > a_j$.

Dacă $\sigma \in \sigma_n$ este o permutare, definim

$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i},$$

$\varepsilon(\sigma)$ se numeşte *semnul* (*signatura*) permutării σ.

Se vede că orice factor $\sigma(j) - \sigma(i)$ (pentru $i < j$), de la numărătorul produsului din expresia lui $\varepsilon(\sigma)$, se simplifică cu unul din factorii de la numitor ce apare eventual cu semn schimbat. Aşadar, $\varepsilon(\sigma)$ este un produs de $+1$ sau -1, mai precis, $\varepsilon(\sigma) = (-1)^{n_\sigma}$, unde n_σ este numărul de inversiuni al permutării σ.

O permutare se numeşte *pară* dacă $\varepsilon(\sigma) = 1$ şi *impară* dacă $\varepsilon(\sigma) = -1$. Este evident că există permutări pare, de exemplu permutarea identică. Vom arăta că există şi permutări impare.

Fie $l, k \in \{1, 2, \ldots, n\}$, $l \neq k$, şi să considerăm permutarea τ_{lk}, definită prin

$$\tau_{lk}(i) = \begin{cases} l, & \text{dacă } i = k, \\ k, & \text{dacă } i = l, \\ i, & \text{dacă } i \neq k \text{ şi } i \neq l. \end{cases}$$

O astfel de permutare se numeşte *transpoziţie*.

Demonstrăm că $\varepsilon(\tau_{lk}) = -1$. Într-adevăr, fie $l < k$. Atunci

$$\tau_{lk} = \begin{pmatrix} 1 & \ldots & l-1 & l & l+1 & \ldots & k-1 & k & k+1 & \ldots & n \\ 1 & \ldots & l-1 & k & l+1 & \ldots & k-1 & l & k+1 & \ldots & n \end{pmatrix}$$

şi numărul de inversiuni este, după cum se constată uşor, $2(k - l) - 1$. Aşadar

$$\varepsilon(\tau_{lk}) = (-1)^{2(k-l)-1} = -1.$$

Propoziţia 7.2. *Aplicaţia*

$$\varepsilon : \sigma_n \to \{1, -1\}, (n \geqslant 2)$$

de la grupul σ_n *la grupul multiplicativ* $\{1, -1\}$ *este un omomorfism surjectiv de grupuri.*

Demonstraţie. Observăm mai întîi că dacă $\sigma, \tau \in \sigma_n$, atunci

$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}$$

şi deci

$$\varepsilon(\sigma\tau) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} =$$

$$= \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \prod_{1 \leqslant i < j \leqslant n} \frac{\tau(j) - \tau(i)}{j - i} = \varepsilon(\sigma)\varepsilon(\tau),$$

adică ε este omomorfism. De mai înainte rezultă că ε este surjectiv.

Nucleul lui ε este un subgrup normal al lui σ_n (vezi § 5) și anume

$$\text{Ker } \varepsilon = \{\sigma \in \sigma_n | \varepsilon(\sigma) = 1\},$$

pe care-l vom nota cu A_n, este format din toate permutările pare ale lui σ_n. A_n se numește *grupul altern de grad n*. Cum ε este surjectiv, conform teoremei de izomorfism la grupuri (vezi teorema 5.4), rezultă

$$\sigma_n/A_n \xrightarrow{\sim} \{1, -1\}.$$

Așadar, conform teoremei lui Lagrange (vezi teorema 4.3), există $\frac{n!}{2}$ permutări pare și deci $\frac{n!}{2}$ permutări impare.

Observație. Dacă $1 \leqslant m \leqslant n$, atunci se poate defini aplicația

$$\varphi_{m,n} : \sigma_m \to \sigma_n$$

prin

$$\varphi_{m,n}(\sigma)(i) = \begin{cases} \sigma(i), & \text{dacă } 1 \leqslant i \leqslant m, \\ i, & \text{dacă } m < i \leqslant n. \end{cases}$$

Se verifică ușor că $\varphi_{m,n}$ este un omomorfism injectiv de grupuri. Acesta ne permite să identificăm grupul σ_m cu un subgrup al lui σ_n și anume cu subgrupul format din acele permutări care lasă invariante numerele $m + 1, \ldots, n$.

Fie $\sigma \in \sigma_n$. Pe mulțimea $\{1, 2, \ldots, n\}$ se definește o relație de echivalență, notată $\overset{\sigma}{\sim}$, în modul următor:

$i \overset{\sigma}{\sim} j$ dacă există $k \in \mathbb{Z}$ astfel încît $\sigma^k(i) = j$, unde

$$\sigma^k = \begin{cases} \underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{(k \text{ factori})}, & \text{dacă } k > 0, \\ e, & \text{dacă } k = 0, \\ \underbrace{\sigma^{-1} \circ \sigma^{-1} \circ \ldots \circ \sigma^{-1}}_{(k \text{ factori})}, & \text{dacă } k < 0. \end{cases}$$

Să verificăm că relația $\overset{\sigma}{\sim}$ este relație de echivalență. Într-adevăr, avem:

1° $i \overset{\sigma}{\sim} i$, deoarece $\sigma^0(i) = e(i) = i$ (e este permutarea identică);

2° dacă $i \overset{\sigma}{\sim} j$, adică $\sigma^k(i) = j$, atunci $\sigma^{-k}(j) = i$ şi deci $j \overset{\sigma}{\sim} i$;

3° dacă $i \overset{\sigma}{\sim} j$ şi $j \overset{\sigma}{\sim} l$, atunci $\sigma^k(i) = j$ şi $\sigma^m(j) = l$ şi deci $\sigma^{k+m}(i) = l$, adică $i \overset{\sigma}{\sim} l$.

Această relaţie de echivalenţă împarte mulţimea $\{1, 2, \ldots, n\}$ în clase de echivalenţă.

Clasele de echivalenţă determinate de relaţia de echivalenţă $\overset{\sigma}{\sim}$ se numesc *orbitele* permutării σ. Dacă o orbită a permutării σ are cel puţin două elemente, aceasta se numeşte *netrivială*.

Definiţia 7.1. O permutare σ se numeşte *ciclu* dacă are o singură orbită netrivială.

Fie σ un ciclu şi $\mathcal{O}_\sigma$ orbita sa netrivială. Atunci card $\mathcal{O}_\sigma$ se numeşte *lungimea ciclului* şi se notează cu $l(\sigma)$.

Dacă $i \notin \mathcal{O}_\sigma$, atunci $\sigma(i) = i$, iar dacă $i_0 \in \mathcal{O}_\sigma$, atunci $\mathcal{O}_\sigma$ este clasa de echivalenţă a lui i_0, adică

$$\mathcal{O}_\sigma = \{j \mid j \overset{\sigma}{\sim} i_0\} = \{\sigma^n(i_0) \mid n \in \mathbb{Z}\}.$$

Fie $\langle\sigma\rangle$ subgrupul generat de σ în $\boldsymbol{\sigma}_n$ şi dacă $m = \text{ord}\, \sigma$, atunci $\langle\sigma\rangle = \{e, \sigma, \sigma^2, \ldots, \sigma^{m-1}\}$. Este uşor de verificat că

$$\mathcal{O}_\sigma = \{i_0, \sigma(i_0), \ldots, \sigma^{m-1}(i_0)\}.$$

Aşadar ord $\sigma = l(\sigma)$.

Fie acum σ un ciclu de lungime m şi

$$\mathcal{O}_\sigma = \{i_0, \sigma(i_0), \ldots, \sigma^{m-1}(i_0)\}.$$

Notăm cu $i_1 = \sigma(i_0)$, $i_2 = \sigma^2(i_0) = \sigma(i_1), \ldots, i_{m-1} = \sigma^{m-1}(i_0) = \sigma(i_{m-2})$ şi evident $\sigma(i_{m-1}) = \sigma^m(i_0) = i_0$. Deci orbita netrivială se scrie

$$\mathcal{O}_\sigma = \{i_0, i_1, \ldots, i_{m-1}\},$$

iar ciclul σ este

$$\sigma = \begin{pmatrix} 1 & \ldots & i_0 - 1 & i_0 & i_1 & \ldots & i_{m-1} & i_m & i_m + 1 & \ldots & n \\ 1 & \ldots & i_0 - 1 & i_1 & i_2 & \ldots & i_m & i_0 & i_m + 1 & \ldots & n \end{pmatrix}$$

pe care îl notăm

$$\sigma = (i_0, i_1, \ldots, i_{m-1}).$$

Un ciclu de lungime 2 este evident o transpoziţie şi reciproc.

Definiția 7.2. Fie σ și τ două cicluri din σ_n, iar $\mathcal{O}_\sigma$ și $\mathcal{O}_\tau$ orbitele netriviale. Dacă $\mathcal{O}_\sigma \cap \mathcal{O}_\tau = \emptyset$, atunci ciclurile σ și τ se numesc *disjuncte*.

Propoziția 7.3. *Orice ciclu $\sigma \in \sigma_n$ este un produs de transpoziții.*

Demonstrație. Fie $\sigma = (i_0, i_1, \ldots, i_{m-1})$. Atunci

$$\sigma = (i_0, i_{m-1}) \ldots (i_0, i_2)(i_0, i_1).$$

Propoziția 7.4. *Dacă $\sigma, \tau \in \sigma_n$ sînt cicluri disjuncte, atunci* $\sigma\tau = \tau\sigma$.

Demonstrație. Fie $i \in \{1, 2, \ldots, n\}$, $i \notin \mathcal{O}_\sigma \cup \mathcal{O}_\tau$; atunci $i \notin \mathcal{O}_\sigma$ și $i \notin \mathcal{O}_\tau$. Deci $\sigma(i) = i$ și $\tau(i) = i$, de unde $(\sigma\tau)(i) = i$ și $(\tau\sigma)(i) = i$. Fie $i \in \mathcal{O}_\sigma \cup \mathcal{O}_\tau$ și $i \in \mathcal{O}_\sigma$, iar $i \notin \mathcal{O}_\tau$. Atunci $(\sigma\tau)(i) = \sigma(\tau(i)) = \sigma(i)$ iar $\tau(\sigma(i)) = \sigma(i)$ și deci $(\sigma\tau)(i) = (\tau\sigma)(i)$. Analog, dacă $i \notin \mathcal{O}_\sigma$, atunci $i \in \mathcal{O}_\tau$.

Teorema 7.5. *Orice permutare $\sigma \in \sigma_n$, $\sigma \neq e$, se descompune ca un produs finit de cicluri disjuncte. Mai mult, această descompunere este unică, abstracție făcînd de ordinea factorilor.*

Demonstrație. Fie $\sigma \neq e$; atunci evident există cel puțin o orbită netrivială. Fie $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ orbitele netriviale ale lui σ. Considerăm $\mathcal{O}_i$ și definim $\tau_i : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ prin

$$\tau_i(j), = \begin{cases} \sigma(j), & \text{dacă } j \in \mathcal{O}_i, \\ j, & \text{dacă } j \notin \mathcal{O}_i. \end{cases}$$

Este clar că τ_i este o permutare și, mai mult, este chiar un ciclu a cărui orbită este $\mathcal{O}_i$. Cum $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ sînt clase de echivalență (deci disjuncte), atunci $\tau_1, \tau_2, \ldots, \tau_r$ sînt cicluri disjuncte. Avem $\sigma = \tau_1\tau_2 \ldots \tau_r$. Într-adevăr, dacă $i \notin \mathcal{O}_1 \cup \mathcal{O}_2 \cup \ldots \cup \mathcal{O}_r$, atunci $\sigma(i) = i$. De asemenea, cum $\tau_k(i) = i$, oricare ar fi $1 \leqslant k \leqslant r$, atunci $(\tau_1\tau_2 \ldots \tau_r)(i) = i$. Dacă $i \in \mathcal{O}_1 \cup \mathcal{O}_2 \cup \ldots \cup \mathcal{O}_r$, atunci există k, $1 \leqslant k \leqslant r$, astfel încît $i \in \mathcal{O}_k$. Dar cum $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ sînt disjuncte, rezultă că $i \notin \mathcal{O}_j$ pentru $j \neq k$. Astfel $\tau_k(i) = \sigma(i)$ și $\tau_j(i) = i$, oricare ar

fi $j \neq k$, deci $(\tau_1 \tau_2 \ldots \tau_r)(i) = \tau_k(i) = \sigma(i)$. Așadar $\sigma(i) = (\tau_1 \tau_2 \ldots \tau_r)(i)$, oricare ar fi $i \in \{1, 2, \ldots, n\}$, deci

$$\sigma = \tau_1\tau_2 \ldots \tau_r.$$

Să demonstrăm unicitatea. Fie pentru aceasta $\sigma = \tau_1\tau_2 \ldots \tau_r = \tau_1' \tau_2' \ldots \tau_s'$ și să arătăm că $r = s$ și, eventual, făcînd o renumerotare a factorilor $\tau_i = \tau_i'$, pentru orice $1 \leqslant i \leqslant r$. Într-adevăr, rezultă imediat că mulțimile de orbite netriviale $\{\mathcal{O}_{\tau_1}, \mathcal{O}_{\tau_2}, \ldots, \mathcal{O}_{\tau_r}\}$ și $\{\mathcal{O}_{\tau_1'}, \mathcal{O}_{\tau_2'}, \ldots, \mathcal{O}_{\tau_s'}\}$ coincid și deci $r = s$. Apoi, eventual, făcînd o renumerotare a orbitelor avem $\mathcal{O}_{\tau_i} = \mathcal{O}_{\tau_i'}$ și deci $\tau_i = \tau_i'$.

Corolarul 7.6. *Orice permutare din σ_n este un produs finit de transpoziții.*

Demonstrație. Avînd în vedere propoziția 7.3 și teorema 7.5, este suficient să observăm că permutarea identică e este produs de transpoziții. Avem evident $e = (1, 2)\ (1, 2)$.

Observație. Descompunerea unei permutări în produs de transpoziții nu este unică, dar conform propoziției 7.2 paritatea numărului de transpoziții care apar în orice descompunere este aceeași. Astfel :

$$e = (1, 2)\,(1, 2) = (1, 2)\,(1, 2)\,(1, 2)\,(1, 2).$$

Exemple. 1. Permutările din σ_2 sînt : e și (1, 2).

2. Permutările din σ_3 sînt : e ; (1, 2) ; (1, 3) ; (2, 3) ; (1, 2, 3) = (1, 3) (1, 2) și (1, 3, 2) = (1, 2) (1, 3).

3. Permutările din σ_4 sînt : permutarea identică, transpoziții, cicluri de lungime 3 și cicluri de lungime 4. Să scriem, de exemplu, pe cele pare care formează grupul altern A_4. Cele 12 permutări ale lui A_4 sînt : e ; (1, 2, 3) = (1, 3) (1, 2) ; (1, 2, 4) = (1, 4) (1, 2) ; (1, 3, 4) = (1, 4) (1, 3) ; (1, 3, 2) = (1, 2) (1, 3) ; (1, 4, 2) = (1, 2) (1, 4) ; (1, 4, 3) = (1, 3) (1, 4) ; (2, 3, 4) = (2, 4) (2, 3) ; (2, 4, 3) = (2, 3)(2, 4) ; (1, 4) (2, 3) ; (1, 3) (2, 4) ; (1, 2) (3, 4).

§ 8. Inel, subinel, ideal

Definiția 8.1. Se numește *inel* o mulțime A înzestrată cu două operații algebrice : $+ : A \times A \to A$ și $\cdot : A \times A \to A$, una notată aditiv și cealaltă multiplicativ, care satisfac următoarele proprietăți :

1) A este grup abelian față de operația aditivă ;

2) operaţia de înmulţire este asociativă;
3) oricare ar fi $x, y, z \in A$, avem

$$(x+y)z = xz + yz, \quad x(y+z) = xy + xz$$

(distributivitatea înmulţirii faţă de adunare).

Într-un inel operaţia aditivă se mai numeşte *adunare* iar cea multiplicativă *înmulţire*.

În cazul unui inel A, grupul abelian A faţă de adunare se numeşte *grupul aditiv al inelului*. Elementul neutru al acestui grup se notează, de obicei, cu 0 şi se numeşte *elementul zero* al inelului, iar opusul faţă de adunare al unui element oarecare $x \in A$ se notează, de obicei, cu $-x$.

Dacă, în plus, operaţia de înmulţire admite element neutru (unitate), se spune că inelul este *cu element unitate* sau *unitar*. Elementul neutru la înmulţire se notează, de obicei, cu 1. Atunci inelul este unitar dacă există un element $1 \in A$, astfel încît

$$x \cdot 1 = 1 \cdot x = x,$$

oricare ar fi $x \in A$. În acest caz, elementul 1 se numeşte *element unitate* sau *unitatea* inelului A.

Dacă înmulţirea este comutativă, adică $xy = yx$, pentru orice $x, y \in A$, inelul se numeşte *comutativ*.

Exemple. 1. Mulţimile $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, cu operaţiile de adunare şi înmulţire, sînt inele.

2. Dacă $n \in \mathbb{Z}$ este un număr întreg, atunci $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ este inel faţă de adunarea şi înmulţirea obişnuită a numerelor întregi.

Propoziţia 8.1. *Într-un inel A sînt adevărate următoarele afirmaţii* :

1) $x0 = 0x = 0$, *oricare ar fi* $x \in A$;

2) $(-x)y = x(-y) = -xy$ şi $(-x)(-y) = xy$, *oricare ar fi* $x, y \in A$.

Demonstraţie. 1) Avem $x0 = x(0+0) = x0 + x0$. Reducînd $x0$ din ambii membri, rezultă $x0 = 0$. De asemenea, se arată că $0 = 0x$.

2) Avem $0 = 0y = (x + (-x))y = xy + (-x)y$. Deci opusul lui xy este $(-x)y$, de unde $(-x)y = -xy$. La fel se arată că $x(-y) = -xy$. În sfîrşit,

$$(-x)(-y) = -(x(-y)) = -(-xy) = xy.$$

O aplicaţie $\varphi : A \to B$, unde A şi B sînt două inele, se numeşte *omomorfism de inele* dacă

$$\varphi(x + y) = \varphi(x) + \varphi(y), \quad \varphi(x\,y) = \varphi(x)\,\varphi(y),$$

oricare ar fi $x, y \in A$.

Dacă A şi B sînt inele unitare şi φ are proprietatea $\varphi(1) = 1$, atunci φ se numeşte *omomorfism unitar*.

Ca şi la grupuri se întîlnesc şi la inele noţiunile corespunzătoare de *omomorfism injectiv*, *omomorfism surjectiv*, *izomorfism*. De asemenea, un omomorfism de inele este izomorfism dacă şi numai dacă este omomorfism bijectiv (vezi propoziţia 2.4).

Un element $x \neq 0$ din inelul comutativ A se numeşte *divizor al lui zero* dacă există $y \neq 0$, $y \in A$, astfel încît $xy = 0$. Un inel unitar, comutativ şi fără divizori ai lui zero se numeşte *domeniu de integritate*. De exemplu, inelul $\mathbb{Z}$ al numerelor întregi este domeniu de integritate.

Un element $a \in A$ (A unitar) se numeşte *inversabil* dacă există $b \in A$ astfel încît $ab = ba = 1$. Un element inversabil nu este divizor al lui zero, deoarece din $ax = 0$ rezultă $bax = 1x = x = 0$.

Definiţia 8.2. Fie A un inel. O submulţime nevidă S a lui A se numeşte *subinel* al lui A dacă S împreună cu operaţiile induse de cele de pe A formează la rîndul său un inel.

Propoziţia 8.2. *Fie A un inel şi $S \subset A$ o submulţime nevidă a sa. Atunci S este un subinel al lui A dacă şi numai dacă:*

1° *oricare ar fi $x, y \in S$, rezultă $x - y \in S$,*

2° *oricare ar fi $x, y \in S$, rezultă $xy \in S$.*

Demonstraţie. Cele două condiţii spun că operaţiile de pe A induc pe S operaţii algebrice. Faptul că S împreună cu acestea formează un inel este uşor de verificat, axiomele de inel pe S fiind adevărate deoarece S este o submulţime a inelului A.

Exemple. 1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sînt subinele unele în altele, cu adunarea şi înmulţirea numerelor.

2. Subinelele lui $\mathbb{Z}$ coincid evident cu subgrupurile grupului aditiv $\mathbb{Z}$, adică sînt de tipul $n\mathbb{Z}$ cu $n \in \mathbb{N}$.

Definiţia 8.3. O submulţime nevidă I a unui inel comutativ A se numeşte *ideal* dacă:

1° $x - y \in I$, oricare ar fi $x, y \in I$;

2° $ax \in I$, oricare ar fi $a \in A$ şi $x \in I$.

Din definiţie rezultă că orice ideal al unui inel este un subinel, pe cînd reciproc nu este adevărat. Astfel, $\mathbb{Z}$ este un subinel al lui $\mathbb{Q}$ dar nu este ideal, deoarece, de exemplu, $2 \in \mathbb{Z}$ şi $\frac{1}{3} \in \mathbb{Q}$, dar $2 \cdot \frac{2}{3} = \frac{4}{3} \notin \mathbb{Z}$.

Exemplu. Idealele inelului $\mathbb{Z}$ coincid evident cu subgrupurile grupului său aditiv, deci sînt de tipul $n\mathbb{Z}$, cu $n \in \mathbb{N}$.

Dacă $\psi : A \to B$ este un omomorfism de inele, atunci mulţimea

$$\operatorname{Ker} \psi = \{x \in A \mid \psi(x) = 0\}$$

este un ideal al lui A.

Într-adevăr, în § 2 s-a demonstrat că Ker ψ este un subgrup al lui A. Fie $a \in A$ şi $x \in \operatorname{Ker} \psi$; atunci $\psi(ax) = \psi(a)\, \psi(x) = \psi(a) \cdot 0 = 0$, deci $ax \in \operatorname{Ker} \psi$.

De asemenea, ψ este un omomorfism injectiv dacă şi numai dacă Ker $\psi = \{0\}$ (vezi propoziţia 2.5).

§ 9. Inel factor. Teorema fundamentală de izomorfism

Fie A un inel comutativ şi I un ideal al său. Avînd în vedere doar structura de grup aditiv a lui A, atunci I este un subgrup aditiv al lui A.

Ca în § 5, introducînd relaţia de echivalenţă următoare: dacă $x, y \in A$, atunci $x \sim y \pmod I$ dacă şi numai dacă $x - y \in I$, se obţine grupul factor A/I. Operaţia algebrică în raport cu care A/I este grup este:

$$\text{dacă } \hat{x}, \hat{y} \in A/I, \text{ atunci } \hat{x} + \hat{y} = \widehat{x+y}.$$

Cum $\hat{x} + \hat{y} = \widehat{x+y} = \widehat{y+x} = \hat{y} + \hat{x}$, rezultă că A/I este un grup abelian. Pe grupul A/I se introduce o nouă operaţie algebrică notată multiplicativ şi anume $\hat{x}\hat{y} = \widehat{xy}$. Această operaţie este bine definită, adică nu depinde de alegerea reprezen-

tanților. Într-adevăr, dacă $x' \in \hat{x}$ și $y' \in \hat{y}$, atunci $x' - x \in I$ și $y' - y \in I$, adică $x' - x = a \in I$ și $y' - y = b \in I$. Deci

$$x'y' = (x + a)(y + b) = xy + xb + ay + ab.$$

Cum I este ideal, rezultă că $xb + ay + ab \in I$ și deci $xy - x'y' \in \in I$, adică $xy \sim x'y'$ (mod I). Așadar

$$\widehat{xy} = \widehat{x'y'}.$$

Lăsăm pe seama cititorului să verifice că dacă A este inel, atunci A/I este inel și, mai mult, dacă A este unitar și A/I este unitar.

Fie acum aplicația canonică

$$p : A \to A/I$$

definită prin $p(x) = \hat{x}$. Din § 5 rezultă că

$$p(x + y) = p(x) + p(y).$$

Dar $p(xy) = \widehat{xy} = \hat{x}\hat{y} = p(x)\,p(y)$ și deci p este un omomorfism de inele.

Inelul A/I se numește *inelul factor* al lui A în raport cu idealul I. Aplicația $p : A \to A/I$ este un omomorfism surjectiv de inele.

Exemplu. Am remarcat mai înainte că idealele lui $\mathbb{Z}$ sînt de tipul $n\mathbb{Z}$ cu $n \geqslant 0$. Deci inelele factor ale lui $\mathbb{Z}$ sînt de forma $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, unde $\mathbb{Z}_0 = \mathbb{Z}$. Inelul $\mathbb{Z}_n$ pentru $n \geqslant 1$ se numește *inelul claselor de resturi modulo n*.

Fie $\varphi : A \to B$ un omomorfism de inele. Atunci Ker φ este un ideal al lui A, iar Im φ este un subinel al lui B.

Teorema 9.1 (*fundamentală de izomorfism*). *Fie* $\varphi : A \to B$ *un omomorfism de inele. Atunci există un izomorfism canonic*

$$\overline{\varphi} : A/\text{Ker}\,\varphi \xrightarrow{\sim} \text{Im}\,\varphi.$$

Demonstrație. Avînd în vedere teorema corespunzătoare pentru grupuri (vezi teorema 5.4), rămîne de verificat doar

faptul că $\overline{\varphi}$ care este definit prin $\overline{\varphi}(\hat{x}) = \varphi(x)$ are proprietatea că $\overline{\varphi}(\hat{x}\hat{y}) = \overline{\varphi}(\hat{x})\,\overline{\varphi}(\hat{y})$. Or

$$\overline{\varphi}(\hat{x}\hat{y}) = \overline{\varphi}(\widehat{xy}) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}(\hat{x})\overline{\varphi}(\hat{y}),$$

oricare ar fi $\hat{x}, \hat{y} \in A/\mathrm{Ker}\ \varphi$. Așadar, $\overline{\varphi}$ este un izomorfism de inele.

§ 10. Inelul claselor de resturi modulo n. Teorema lui Euler

În acest paragraf demonstrăm unele proprietăți ale inelelor $\mathbb{Z}_n$ și dăm cîteva aplicații ale acestora.

Propoziția 10.1. *Fie $n \geqslant 2$ și $\mathbb{Z}_n$ inelul claselor de resturi modulo n. Un element $\hat{x}$ din $\mathbb{Z}_n$ este inversabil dacă și numai dacă x este prim cu n. În particular, dacă n este prim, orice element nenul din $\mathbb{Z}_n$ este inversabil.*

Demonstrație. Fie $\hat{x} \in \mathbb{Z}_n$ și $(x, n)=1$. Atunci există $a, b \in \mathbb{Z}$ astfel încît $xa + nb = 1$, de unde, trecînd la clase, rezultă $\hat{x}\hat{a}=\hat{1}$ și deci $\hat{x}$ este inversabil. Reciproc, dacă $\hat{x}$ este inversabil, rezultă că există $\hat{c} \in \mathbb{Z}_n$ astfel încît $\hat{x}\hat{c} = \hat{1}$. Deci $xc \equiv 1(\mathrm{mod}\ n)$, adică există $d \in \mathbb{Z}$ astfel încît $xc - 1 = dn$, de unde $xc - dn = 1$, ceea ce spune că $(x, n) = 1$.

În particular, cînd n este prim, rezultă că orice element nenul din $\mathbb{Z}_n$ este inversabil.

Observația 1. Dacă A și B sînt două inele, atunci pe produsul cartezian al mulțimilor subiacente lui A și B, adică pe

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

se poate introduce în mod natural o structură de inel. Mai precis, dacă (a, b), $(a', b') \in A \times B$, atunci punem

$$(a, b) + (a', b') = (a + a', b + b') \text{ și } (a, b)(a', b') = (aa', bb').$$

Lăsăm cititorului verificarea faptului că $A \times B$ cu aceste două operații este un inel. Acest inel se numește *produsul* inelelor A și B.

În particular, dacă m și n sînt două numere $\geqslant 1$, se obține inelul produs $\mathbb{Z}_m \times \mathbb{Z}_n$.

Propoziția 10.2. *Dacă m, n sînt două numere întregi $\geqslant 2$, prime între ele, atunci inelul $\mathbb{Z}_m \times \mathbb{Z}_n$ este izomorf cu $\mathbb{Z}_{mn}$.*

Demonstrație. Fie $\varphi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ aplicația definită prin $\varphi(\hat{\hat{x}}) = (\hat{x}, \bar{x})$, unde prin $\hat{\hat{x}}$ (respectiv $\hat{x}$, $\bar{x}$) s-a notat clasa de resturi modulo mn (respectiv m, n). Să arătăm mai întîi că φ este bine definită. Într-adevăr, dacă $\hat{\hat{x}} = \hat{\hat{y}}$, atunci $mn \mid x - y$ și cum $(m, n) = 1$, rezultă că $m \mid x - y$ și $n \mid x - y$, adică $\hat{x} = \hat{y}$ și $\bar{x} = \bar{y}$. Așadar, $\varphi(\hat{\hat{x}}) = \varphi(\hat{\hat{y}})$.

Dacă $\varphi(\hat{\hat{x}}) = \varphi(\hat{\hat{y}})$, atunci $(\hat{x}, \bar{x}) = (\hat{y}, \bar{y})$, adică $\hat{x} = \hat{y}$ și $\bar{x} = \bar{y}$ și deci $m \mid x - y$ și $n \mid x - y$. Cum $(m, n) = 1$, rezultă $mn \mid x - y$, adică $\hat{\hat{x}} = \hat{\hat{y}}$ și deci φ este injectivă. Întrucît $\mathbb{Z}_m \times \mathbb{Z}_n$ și $\mathbb{Z}_{mn}$ au același număr de elemente și φ este injectivă, rezultă că φ este bijectivă. Faptul că φ este un omomorfism de inele rezultă dintr-un calcul simplu. Deci φ este izomorfism de inele.

Observația 2. Fie A și B două inele unitare și $A \times B$ inelul produs. Dacă $(a, b) \in A \times B$ este inversabil, atunci există $(a', b') \in A \times B$ astfel încît $(a, b)(a', b') = (a', b')(a, b) = (1, 1)$ și deci $(aa', bb') = (a'a, b'b) = (1, 1)$, adică $aa' = a'a = 1$ și $bb' = b'b = 1$. Prin urmare, a și b sînt inversabile. Reciproc, dacă $a \in A$ și $b \in B$ sînt inversabile, atunci $(a, b) \in A \times B$ este inversabil.

Definiția 10.1. Fie $n > 1$ un număr natural; notăm cu $\varphi(n)$ numărul numerelor naturale nenule mai mici decît n și prime cu n. Acest număr se numește *indicatorul lui Euler*.

Propoziția 10.3. *Dacă m și n sînt două numere naturale > 1, prime între ele, atunci*

$$\varphi(mn) = \varphi(m)\, \varphi(n).$$

Demonstrația rezultă după propozițiile 10.1, 10.2 și observația 2.

Teorema 10.4 (*Euler*). *Fie n un număr natural > 1 și a un număr întreg prim cu n. Atunci*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Demonstrație. Mulțimea elementelor inversabile din $\mathbb{Z}_n$, față de înmulțire, formează un grup $U(\mathbb{Z}_n)$ care are ordinul egal cu $\varphi(n)$. Fie acum $a \in \mathbb{Z}$, $(a, n) = 1$. Atunci $\hat{a} \in U(\mathbb{Z}_n)$ și conform teoremei lui Lagrange $\mathrm{ord}(\hat{a}) \mid \mathrm{ord}\, U(\mathbb{Z}_n)$, adică $\mathrm{ord}\, \hat{a} \mid \varphi(n)$. Așadar $\hat{a}^{\varphi(n)} = \hat{1}$, de unde $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Corolarul 10.5 (*teorema lui Fermat*). *Dacă $p > 1$ este un număr natural prim și a un număr întreg care nu se divide cu p, atunci*

$$a^{p-1} \equiv 1 \pmod p.$$

Demonstrația rezultă din teorema lui Euler ținînd seama de faptul că dacă p este prim, după propoziția 10.1, avem $\operatorname{ord} U(\mathbb{Z}_p) = p - 1$.

Dăm, în final, o formulă de calcul al lui $\varphi(n)$.

Propoziția 10.6. *Fie $n > 1$ un număr întreg și $n = p_1^{k_1} p_2^{k_2} \ldots$ $\ldots p_r^{k_r}$ descompunerea sa în produs de numere prime, unde $p_1, p_2, \ldots, p_r$ sînt distincte. Atunci*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right).$$

Demonstrație. Fie mai întîi $n = p^k$, cu $k \geqslant 1$ și p prim. Scriem numerele mai mici ca p^k:

$$0, 1, 2, \ldots, p, p + 1, \ldots, 2p, 2p + 1, \ldots, p^k - 1.$$

Aici, din p în p termenii sînt numere multipli de p. Deci $\frac{p^k}{p} = p^{k-1}$ numere $< p^k$ nu sînt prime cu p și deci $p^k - p^{k-1}$ sînt prime cu p. Așadar $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$.

Fie $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$. Făcînd inducție după n și avînd în vedere propoziția 10.3, este clar că

$$\varphi(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \ldots \varphi(p_r^{k_r}).$$

Dar cum $\varphi(p_i^{k_i}) = p_i^{k_i}\left(1 - \frac{1}{p_i}\right)$, rezultă evident

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right).$$

§ 11. Corp, subcorp

Definiția 11.1. Uninel unitar K cu $1 \neq 0$ se numește *corp* dacă orice element nenul din K este inversabil față de înmulțire.

Deci, K este corp dacă :

1) K este inel unitar ;

2) oricare $x \in K$, $x \neq 0$, există $x^{-1} \in K$ astfel încît

$$xx^{-1} = x^{-1}x = 1.$$

Aşadar, inelul unitar K este un corp dacă mulţimea K^* a elementelor nenule din K formează faţă de înmulţire un grup. În plus, dacă înmulţirea este comutativă se spune că corpul este *comutativ*.

Exemple. Mulţimile de numere $\mathbb{Q}$, $\mathbb{R}$ şi $\mathbb{C}$ împreună cu operaţiile de adunare şi înmulţire formează corpuri comutative. După propoziţia 10.1, dacă p este un număr prim, atunci inelul $\mathbb{Z}_p$ al claselor de resturi modulo p este un corp.

Toate corpurile considerate mai jos sînt comutative.

Definiţia 11.2. Dacă K este un corp, o submulţime nevidă F a lui K este un *subcorp* al lui K dacă operaţiile algebrice de pe K induc pe F operaţii algebrice faţă de care F este un corp. Dacă F este un subcorp al lui K, atunci K se numeşte *extindere* a lui F.

Propoziţia 11.1. *Fie K un corp şi $F \subset K$ o submulţime nevidă a sa. Atunci F este un subcorp al lui K, dacă şi numai dacă :*

1° $x - y \in F$, *oricare ar fi* $x, y \in F$;

2° $xy^{-1} \in F$, *oricare ar fi* $x, y \in F$, $y \neq 0$.

Demonstraţie. Echivalenţa celor două afirmaţii din propoziţie este imediată.

Observăm că elementul unitate din K este element unitate pentru F. De asemenea, după cum am observat în § 8, un corp K este domeniu de integritate (adică nu are divizori ai lui zero).

Dacă K şi K' sînt două corpuri, atunci un *omomorfism* de corpuri de la K la K' este o aplicaţie $\varphi : K \to K'$, astfel încît

$$\varphi(x + y) = \varphi(x) + \varphi(y),$$
$$\varphi(xy) = \varphi(x)\,\varphi(y), \text{ oricare ar fi } x, y \in K,$$
$$\varphi(1) = 1.$$

Deci $\varphi : K \to K'$ este un omomorfism de corpuri dacă este un omomorfism unitar de inele.

Cum φ este, în particular, un omomorfism al grupului multiplicativ K^* în K'^*, rezultă $\varphi(x^{-1}) = (\varphi(x))^{-1}$, pentru orice $x \neq 0$. De asemenea, din $\varphi(x) = \varphi(y)$ avem $\varphi(x - y) = 0$

și deci $x - y = 0$, adică $x = y$, deoarece în caz contrar, dacă $x - y \neq 0$, există $z \in K$ astfel încît $(x - y)z = 1$, de unde

$$1 = \varphi(1) = \varphi((x - y)z) = \varphi(x - y)\ \varphi(z) = 0,$$

ceea ce reprezintă contradicție.

Fie K un corp comutativ. Atunci ordinul elementului $1 \in K$, în grupul aditiv $(K, +)$, poate fi finit sau infinit. Se spune că corpul K *are caracteristica zero* (sau este de caracteristică zero) dacă ord (1) este infinit, adică $m \cdot 1 \neq 0$, pentru orice număr întreg pozitiv m. Se spune că corpul K este *de caracteristică* n, dacă ord $(1) = n$, adică n este cel mai mic număr întreg pozitiv astfel încît $n \cdot 1 = 0$.

Propoziția 11.2. *Caracteristica unui corp K este* 0 *sau un număr prim.*

Demonstrație. Dacă $n =$ ord (1) este finit, dar nu este prim, atunci $n = pq$ cu $1 < p < n$ și $1 < q < n$, iar $0 = n \cdot 1 = (p \cdot q)1 = (p \cdot 1)(q \cdot 1)$. Cum K este corp, deci nu are divizori ai lui zero, atunci $p \cdot 1 = 0$ sau $q \cdot 1 = 0$, ceea ce contrazice alegerea lui n.

Observăm că dacă $E \supset K$ este o extindere a unui corp K, atunci E și K au aceeași caracteristică.

Exemple. Dacă p este număr prim, atunci $\mathbb{Z}_p$ este un corp care are caracteristica p. Corpurile $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ au caracteristica zero.

Următoarele egalități sînt adevărate într-un corp K de caracteristică p:

$$px = 0,\ (x \pm y)^p = x^p \pm y^p,\ (xy)^p = x^p y^p$$

pentru orice $x, y \in K$.

Într-adevăr, prima din această relație reiese din egalitățile $px = p(1 \cdot x) = (p \cdot 1)x = 0 \cdot x = 0$. A doua rezultă din faptul că dacă p este un număr prim, coeficienții binomiali C_p^k, $1 \leqslant k \leqslant p - 1$, sînt multipli de p. Atunci, din relația precedentă avem că $(x \pm y)^p = x^p + (\pm 1)^p y^p$. Dacă $p \neq 2$, atunci p este impar și deci $(x \pm y)^p = x^p \pm y^p$. Dacă $p = 2$, avem $(x - y)^2 = x^2 + y^2$, însă în același timp $y^2 = -y^2$, deoarece $2y^2 = 0$. Ultima relație este evidentă. Observăm că, din ultimele două relații rezultă că aplicația $x \to x^p$ este un endomorfism al corpului K.

§ 12. Corpul de fracții al unui domeniu de integritate

Fie K un corp comutativ. Orice subinel al său este un domeniu de integritate. Problema care o punem este inversa acesteia și anume, fiind dat un domeniu de integritate A, să găsim un corp K astfel încît A să fie subinel al lui K.

Fie deci A un domeniu de integritate și A^* mulțimea elementelor nenule ale lui A. Considerăm produsul de mulțimi:

$$A \times A^* = \{(a, b) | a \in A, \ b \in A^*\}.$$

Pe $A \times A^*$ se introduce o relație de echivalență R definită astfel:

$$(a, b)R(c, d) \text{ dacă și numai dacă } ad = bc.$$

Să verificăm că R este relație de echivalență. Într-adevăr, $(a, b)R(a, b)$, deoarece $ab = ba$; dacă $(a, b)R(c, d)$, atunci $ad = bc$ și deci $cb = da$, adică $(c, d)R(a, b)$. În sfîrșit, dacă $(a, b)R(c, d)$ și $(c, d)R(e, f)$, atunci $ad = bc$ și $cf = de$. Prin urmare, $adf = bcf = bde$ și cum $d \neq 0$, iar A este domeniu de integritate, $af = be$, adică $(a, b)R(e, f)$. Deci R este relație de echivalență.

Clasa de echivalență a perechii (a, b) se numește *fracție* și se notează prin $\frac{a}{b}$. Atunci avem $\frac{a}{b} = \frac{c}{d}$ dacă și numai dacă $ad = bc$.

Fie $K = (A \times A^*)/R$ mulțimea factor a lui $A \times A^*$ în raport cu relația de echivalență R. Pe această mulțime se introduc două operații algebrice (adunarea și înmulțirea) în raport cu care K devine un corp.

Fie $\frac{a}{b}$, $\frac{c}{d}$ două fracții. Cum $b \neq 0$ și $d \neq 0$, atunci $bd \neq 0$ și deci are sens fracția $\frac{ad + bc}{bd}$.

Dacă $\frac{a}{b} = \frac{a'}{b'}$ și $\frac{c}{d} = \frac{c'}{d'}$, atunci

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}.$$

Într-adevăr, avem $ab' = ba'$ și $cd' = dc'$. Deci $ab'dd' = ba'dd'$ și $cd'bb' = dc'bb'$, de unde $ab'dd' + cd'bb' = ba'dd' + dc'bb'$, sau încă $(ad + bc)\, b'd' = (a'd' + b'c')\, bd$, ceea ce trebuia demonstrat.

Atunci definim *adunarea* prin

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

operație care este bine definită (nu depinde de alegerea reprezentanților), după cum am văzut mai sus.

Înmulțirea o definim prin:

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$$

care se verifică ușor că este bine definită.

Punem $0=\frac{0}{1}$ și $1=\frac{1}{1}$. Lăsăm cititorului să verifice următoarele: K împreună cu adunarea și înmulțirea definite mai sus este un inel unitar.

Fie $\frac{a}{b}\neq 0$ din K; atunci $a\neq 0$. Deci are sens fracția $\frac{b}{a}$ care este din K și $\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ba}=\frac{1}{1}=1$. Prin urmare, orice element $\frac{a}{b}\neq 0$ din K are un invers și anume $\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$. Deci K este un corp comutativ.

Fie aplicația $j: A\to K$ definită prin $j(a)=\frac{a}{1}$. Avem

$$j(a+b)=\frac{a+b}{1}=\frac{a}{1}+\frac{b}{1}=j(a)+j(b)$$

și

$$j(ab)=\frac{ab}{1}=\frac{a}{1}\frac{b}{1}=j(a)j(b).$$

Deci j este un omomorfism. Dacă $j(a)=0$, adică $\frac{a}{1}=0=\frac{0}{1}$, atunci $a\cdot 1=1\cdot 0=0$, adică $a=0$. Prin urmare, $\operatorname{Ker} j=\{0\}$, adică j este omomorfism injectiv.

Acest omomorfism injectiv permite identificarea lui A cu un subinel al lui K, mai precis, $a=\frac{a}{1}$. Atunci, dacă $\frac{a}{b}\in K$, putem scrie $\frac{a}{b}=\frac{a}{1}\frac{1}{b}=\frac{a}{1}\left(\frac{b}{1}\right)^{-1}=ab^{-1}$. Corpul K se numește *corpul fracțiilor* (sau *corpul de fracții*) al lui A.

Exemplu. Pentru $A=\mathbb{Z}$, inelul numerelor întregi, prin procedeul descris, se obține corpul $\mathbb{Q}$ al fracțiilor raționale. În cap. III, § 6, se întîlnește un alt exemplu de corp de fracții al unui domeniu de integritate.

III

INELE DE POLINOAME

§ 1. Construcția inelului de polinoame într-o nedeterminată. Proprietăți generale

Fie A un inel comutativ și unitar. Se va da o construcție a inelului de polinoame într-o nedeterminată peste A care, la început, nu folosește scrierea obișnuită a polinoamelor cu ajutorul unei „nedeterminate" X.

Pentru inelul A, se consideră șirurile

$$f = (a_0, a_1, a_2, \dots), \ a_i \in A,$$

astfel încît toți termenii a_i, în afară de un număr finit dintre ei, sînt nuli. Fie A' mulțimea tuturor șirurilor de acest tip. Șirurile $f = (a_0, a_1, a_2, \dots)$ și $g = (b_0, b_1, b_2, \dots)$ sînt egale dacă și numai dacă $a_i = b_i$, pentru orice i.

Pe mulțimea A' se definesc două operații algebrice, *adunarea* și *înmulțirea*, în raport cu care A' devine un inel comutativ și unitar.

Fie $f, g \in A'$,

$$f = (a_0, a_1, a_2, \dots), \quad g = (b_0, b_1, b_2, \dots);$$

atunci adunarea se definește astfel:

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots).$$

Este evident că $f + g$ are numai un număr finit de termeni nenuli, deci $f + g \in A'$.

Se verifică ușor că A' împreună cu adunarea este un grup abelian, adică adunarea este asociativă, comutativă, are element nul și orice element are un opus. Elementul nul (zero) este

$$(0, 0, 0, \dots).$$

Dacă $f = (a_0, a_1, a_2, \dots)$ este un element din A', atunci opusul său este

$$-f = (-a_0, -a_1, -a_2, \dots).$$

Înmulțirea pe A' se definește astfel:

$$fg = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \dots) = (c_0, c_1, c_2, \dots),$$

unde

$$c_k = \sum_{i+j=k} a_ib_j, \ k = 0, 1, 2, \dots$$

Este clar că $fg \in A'$. Înmulțirea pe A' astfel definită este asociativă, comutativă și are element unitate. Să arătăm, mai întîi, asociativitatea.

Fie $f, g, h \in A'$, unde

$$f = (a_0, a_1, a_2, \dots), \ g = (b_0, b_1, b_2, \dots), \ h = (c_0, c_1, c_2, \dots)$$

și să arătăm că $(fg)h = f(gh)$. Fie $fg = (d_0, d_1, d_2, \dots)$. Atunci $d_k = \sum_{i+j=k} a_ib_j$. De asemenea, fie $(fg)h = (d'_0, d'_1, d'_2, \dots)$, unde

$$d'_m = \sum_{k+l=m} d_kc_l = \sum_{k+l=m} \left(\sum_{i+j=k} a_ib_j \right) c_k = \sum_{\substack{k+l=m \\ i+j=k}} a_ib_jc_k = \sum_{i+j+l=m} a_ib_jc_l.$$

Dacă $gh = (e_0, e_1, e_2, \dots)$, atunci $e_i = \sum_{i+j=l} b_ic_j$ și fie

$$f(gh) = (e'_0, e'_1, e'_2, \dots),$$

unde

$$e'_m = \sum_{k+l=m} a_k e_l = \sum_{k+l=m} a_k \Big(\sum_{i+j=l} b_i c_j\Big) = \sum_{\substack{k+l=m\\ i+j=l}} a_k b_i c_j = \sum_{k+i+j=m} a_k b_i c_j.$$

Deci $d'_m = e'_m$ pentru orice m.

Comutativitatea înmulțirii rezultă din faptul că înmulțirea în inelul A este comutativă iar în expresia termenilor produsului polinoamelor f și g termenii factorilor intervin în mod simetric.

Elementul unitate din A' este șirul $(1, 0, 0, \ldots)$.

Mai mult, înmulțirea pe A' este distributivă, față de adunare. Într-adevăr, cu notațiile de mai sus, rezultă

$$f(g + h) = (d_0, d_1, d_2, \ldots), \text{ unde } d_k = \sum_{i+j=k} a_i(b_j + c_j);$$

$$fg + fh = (d'_0, d'_1, d'_2, \ldots), \text{ unde } d'_k = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j.$$

Cum operația de înmulțire pe A este distributivă față de adunare, rezultă

$$f(g + h) = fg + fh.$$

Evident, are loc și relația

$$(f + g)h = fh + gh.$$

În concluzie, s-a demonstrat :

Propoziția 1.1. *Dacă A este un inel unitar comutativ, atunci mulțimea A' (a șirurilor de elemente din A, care au numai un număr finit de termeni nenuli) împreună cu operațiile de adunare și înmulțire definite mai sus este un inel comutativ și unitar.*

Elementele acestui inel se numesc *polinoame peste A*, sau *polinoame cu coeficienți din A*.

Dacă $f = (a_0, a_1, a_2, \ldots)$ este un polinom nenul (adică nu toți termenii a_i sînt nuli) și dacă n este cel mai mare număr natural cu proprietatea că $a_n \neq 0$, atunci n se numește *gradul polinomului f*. Gradul polinomului f va fi notat prin grad (f). Pentru polinomul nul nu se definește gradul. Convenim, în

schimb, să considerăm gradul său ca fiind $-\infty$, adoptînd convențiile uzuale și anume : $-\infty < n$ pentru orice număr natural n, $-\infty + (-\infty) = -\infty$, $-\infty + n = -\infty$. Dacă grad $(f) = n$, atunci a_0, a_1, a_2, $\ldots$, a_n se numesc *coeficienții* polinomului f.

Fie aplicația $u : A \to A'$ definită prin

$$u(a) = (a, 0, 0, \ldots).$$

Cum $(a, 0, 0, \ldots) = (b, 0, 0, \ldots)$ implică $a = b$, rezultă că u este injectivă. Mai mult, u este un omomorfism de inele. Într-adevăr, avem $u(a + a') = u(a) + u(a')$ și $u(aa') = u(a)u(a')$, oricare ar fi a, $a' \in A$, deoarece, după definiție, este evident că

$$(a, 0, 0, \ldots) + (a', 0, 0, \ldots) = (a + a', 0, 0, \ldots),$$

$$(a, 0, 0, \ldots)(a', 0, 0, \ldots) = (aa', 0, 0, \ldots).$$

Deci u este un omomorfism injectiv. Acest fapt permite să se identifice elementul a din A cu imaginea sa prin u, adică cu polinomul $(a, 0, 0, \ldots)$ din A'. Astfel A se poate considera ca un subinel al lui A'.

Pe de altă parte, se notează prin X polinomul $(0, 1, 0, \ldots)$, care se numește *nedeterminata* X. După înmulțirea definită mai sus se obține $X^2 = (0, 0, 1, 0, \ldots)$ și, mai general, pentru orice număr natural i

$$X^i = (\underbrace{0, 0, \ldots, 0}_{i \text{ ori}}, 1, 0, \ldots).$$

Fie un polinom f de grad n ai cărui coeficienți sînt a_0, a_1, $a_2, \ldots, a_n$, adică $f = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$. Folosind adunarea și înmulțirea definite pe A', se obține

$$f = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots) = (a_0, 0, \ldots) + (0, a_1, 0, \ldots) +$$

$$+ (0, 0, a_2, 0, \ldots) + \ldots + (0, 0, \ldots, 0, a_n, 0, \ldots) = (a_0, 0, 0, \ldots) +$$

$$+ (a_1, 0, 0, \ldots)(0, 1, 0, \ldots) + (a_2, 0, 0, \ldots)(0, 0, 1, 0 \ldots) + \ldots$$

$$\ldots + (a_n, 0, 0, \ldots)(\underbrace{0, 0, \ldots, 0}_{n \text{ ori}}, 1, 0, \ldots);$$

ceilalţi termeni fiind nuli, nu-i mai scriem. Mai mult, după notaţiile indicate, f se poate scrie încă :

$$f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n.$$

Astfel, am obţinut scrierea obişnuită a polinoamelor.

Inelul A' obţinut mai sus se numeşte *inelul polinoamelor* în nedeterminata X, cu coeficienţi în inelul A (sau peste inelul A) şi se notează prin $A[X]$.

$A[X]$ se mai numeşte şi *inelul polinoamelor într-o nedeterminată.* Observăm că f are gradul 0 sau $-\infty$ dacă şi numai dacă f aparţine inelului A, iar grad $(f) = 0$ dacă şi numai dacă f este un element nenul al lui A. Din definiţia sumei şi produsului a două polinoame rezultă că :

$$\text{grad}\,(f + g) \leqslant \max\,(\text{grad}\,(f), \text{grad}\,(g)),$$

$$\text{grad}\,(fg) \leqslant \text{grad}\,(f) + \text{grad}\,(g)$$

pentru orice f, g din $A[X]$. Dacă A este domeniu de integritate, se poate înlocui a doua inegalitate printr-o egalitate. Mai mult, avem

Propoziţia 1.2. *Dacă A este un domeniu de integritate, atunci inelul de polinoame $A[X]$ este domeniu de integritate.*

Demonstraţie. Fie f şi g două polinoame din $A[X]$:

$$f = a_0 + a_1X + a_2X^2 + \ldots + a_mX^m, \quad a_m \neq 0,$$

$$g = b_0 + b_1X + b_2X^2 + \ldots + b_nX^n, \quad b_n \neq 0.$$

Atunci

$$fg = a_0b_0 + (a_0b_1 + a_1b_0)X + \ldots + (a_{m}\cdot\, b_n + a_mb_{n-1})\, X^{m+n-1} +$$
$$+ a_mb_nX^{m+n}.$$

A fiind domeniu de integritate, rezultă $a_mb_n \neq 0$ şi deci $fg \neq 0$.

În particular, pentru un corp comutativ K, inelul polinoamelor de o nedeterminată cu coeficienţi în K este inel integru.

Propoziţia 1.3. *Fie A un domeniu de integritate şi $A[X]$ inelul polinoamelor într-o nedeterminată cu coeficienţi în A. Atunci elementele inversabile ale inelului $A[X]$ coincid cu elementele inversabile ale inelului A.*

Demonstraţie. Fie $a \in A$, inversabil în A, adică există $b \in A$ astfel încît $ab = 1$. Evident această relaţie are loc şi în $A[X]$, deci a este inversabil în $A[X]$. Invers, fie f un polinom din $A[X]$ inversabil. Atunci există un polinom g, astfel încît $fg = 1$ şi deci $\text{grad}(f) + \text{grad}(g) = \text{grad}(1) = 0$, de unde $\text{grad}(f) = \text{grad}(g) = 0$, adică $f, g \in A$. Deci $f \in A$ şi f este inversabil în A.

În particular, pentru un corp comutativ K, polinoamele inversabile din $K[X]$ sînt polinoamele de grad zero şi numai acestea.

Fie A, B două inele comutative şi unitare, astfel încît A este subinel al lui B şi fie $f = a_0 + a_1X + \ldots + a_nX^n$ un polinom oarecare din $A[X]$. Pentru $y \in B$ punem $f(y) = a_0 + a_1y + \ldots + a_ny^n$. Atunci $f(y) \in B$ iar $f(y)$ este *valoarea* polinomului f pentru $X = y$. Se spune că elementul $y \in B$ anulează polinomul $f \in A[X]$ sau că y este o *rădăcină* sau un *zero* al lui f dacă $f(y) = 0$.

Propoziţia 1.4. *Fie A un subinel comutativ şi unitar al inelului comutativ şi unitar B. Dacă $y \in B$ este un element oarecare fixat al lui B, atunci aplicaţia $f \to f(y)$ este un omomorfism de inele de la $A[X]$ la B.*

Demonstraţie. Să notăm cu $\varphi : A[X] \to B$ aplicaţia $\varphi(f) = f(y)$. Trebuie să demonstrăm că

$$\varphi(f + g) = \varphi(f) + \varphi(g) \text{ şi } \varphi(fg) = \varphi(f)\cdot\varphi(g),$$

adică

$$(f + g)(y) = f(y) + g(y), \ (fg)(y) = f(y)\,g(y)$$

pentru orice două polinoame f, g din $A[X]$.

Dacă $f = a_0 + a_1X + \ldots + a_mX^m$ şi $g = b_0 + b_1X + \ldots + b_nX^n$, relaţiile devin

$$\sum (a_i + b_i)\,y^i = \sum a_iy^i + \sum b_iy^i,$$

$$\sum c_ky^k = (\sum a_iy^i)(\sum b_iy^i), \text{ unde } c_k = \sum_{i+j=k} a_ib_j.$$

Dar aceste relații rezultă imediat după definiția adunării și înmulțirii polinoamelor.

Dacă însă fixăm polinomul f din $A[X]$, aplicația $y \to f(y)$, $y \in B$, este o aplicație a inelului B în el însuși. Să notăm această funcție prin f_B. Astfel, fiecărui polinom f din $A[X]$ și fiecărui inel B care conține pe A îi corespunde o funcție definită pe B cu valori în B.

Orice aplicație de la B în B care poate fi pusă sub forma unei funcții f_B pentru un anumit f din $A[X]$ se numește *funcție polinomială* pe B sau *funcție asociată polinomului* f. Cea mai mare parte a funcțiilor de la B la B nu sînt funcții polinomiale. De exemplu, dacă B este corpul numerelor reale, funcția exponențială $x \to e^x$ nu este o funcție polinomială.

Observăm că, dat fiind un inel B ce conține pe A, pot exista polinoame diferite care dau aceeași funcție polinomială pe B, cu alte cuvinte, există un polinom nenul f, astfel încît $f(y) = 0$, pentru toți $y \in B$. De exemplu, dacă $B = A$ este un inel care are doar un număr finit de elemente, fie acestea $a_1, a_2, \ldots, a_n$, putem lua $f = (X - a_1)(X - a_2) \ldots (X - a_n)$; evident, $f(y) = 0$ pentru orice $y \in A$. Pe de altă parte, există inele B care conțin pe A, pentru care $f_B \neq g_B$ dacă $f \neq g$. Cel mai simplu exemplu de astfel de inel se obține dacă luăm $B = A[X]$ deoarece avem $f(X) = f \neq g = g(X)$.

Dacă $f = a \in A$, atunci funcția f_B este constantă; $f_B(y) = a$ pentru orice $y \in B$. Din acest motiv elementele inelului A, considerate ca polinoame, se vor numi *polinoame constante*. Avînd în vedere cele spuse mai sus, pot fi funcții polinomiale f_B care să fie constante, chiar cînd $f \notin A$. Dar numai acele polinoame care sînt în A se numesc constante.

§ 2. Proprietăți aritmetice ale inelelor de polinoame

Prezentăm o extensie a algoritmului de împărțire a polinoamelor cu coeficienți într-un corp.

Teorema 2.1 (*a împărțirii cu rest*). *Fie A un domeniu de integritate, f, $g \neq 0$ două polinoame din $A[X]$ astfel încît coeficientul termenului de grad maxim al lui g să fie inversabil în A. Atunci există polinoamele q și r din $A[X]$, unic determinate, astfel încît*

$$f = gq + r \text{ și } \operatorname{grad}(r) < \operatorname{grad}(g).$$

Demonstrație. Procedăm prin inducție după gradul lui f. Fie m gradul lui f iar n gradul lui g. Dacă grad $(f) = m < n =$ $=$ grad (g), atunci $q = 0$ și $r = f$. Dacă $m \geqslant n$, fie a_m și b_n coeficienții termenilor de grad maxim al lui f, respectiv al lui g. Prin ipoteză b_n este inversabil. Atunci fie

$$f - (a_m b_n^{-1}) X^{m-n} g = f_1.$$

Deoarece coeficienții lui X^m în f și în $(a_m b_n^{-1}) X^{m-n} g$ sînt egali, este clar că grad $(f_1) <$ grad (f). Prin urmare, după ipoteza inducției, există polinoamele q_1 și r_1 din $A[X]$ astfel încît

$$f_1 = g q_1 + r_1, \text{ unde grad } (r_1) < \text{grad } (g).$$

Atunci

$$f = a_m b_n^{-1} X^{m-n} g + g q_1 + r_1 = g(a_m b_n^{-1} X^{m-n} + q_1) + r_1,$$

unde grad $(r_1) <$ grad (g). Deci, $f = gq + r$, unde grad $(r) <$ $<$ grad (g), $q = a_m b_n^{-1} X^{m-n} + q_1$ iar $r = r_1$.

Să demonstrăm unicitatea lui q și r. Într-adevăr, dacă avem încă $f = gq' + r'$, unde grad $(r') <$ grad (g), atunci rezultă $g(q - q_1) = r' - r$, unde grad $(r' - r) <$ grad (g) și $g \neq 0$. Cum b_n este inversabil, deci nu este divizor al lui zero în A, dacă $q \neq q'$, rezultă că grad $(g(q - q')) \geqslant$ grad (g). Așadar, gradul polinomului din membrul întîi al egalității $g(q - q') = r' - r$ este $\geqslant n$, iar al celui din membrul al doilea este $< n$ și se obține contradicție. Deci, în mod necesar $q = q'$ și $r = r'$. Polinomul r poate fi nul (în acest caz, după convenția făcută, gradul său este $-\infty$).

Din această teoremă rezultă evident :

Corolarul 2.2. *Fie K un corp comutativ și f, $g \neq 0$ două polinoame din $K[X]$. Atunci există polinoamele q și r din $K[X]$, unic determinate, astfel încît*

$$f = gq + r \text{ și grad } (r) < \text{grad } (g).$$

Polinomul q se numește *cîtul* împărțirii lui f la g iar r, *restul* împărțirii.

Vom da acum cîteva fapte referitoare la divizibilitate în inele de polinoame. Presupunem în cele ce urmează că A este

un domeniu de integritate. Atunci $A[X]$ este domeniu de integritate (vezi propoziția 1.2).

Fie f și g două polinoame din $A[X]$. Spunem că *f divide g* (în inelul $A[X]$) dacă există $h \in A[X]$ astfel încît $g = fh$. Dacă f divide g, scriem $f|g$; în caz contrar, spunem că *f nu divide g* în inelul $A[X]$. Cînd f divide g, se mai spune că *g se divide prin f* sau că g este un *multiplu* de f, sau, încă, f este un *divizor* al lui g (în inelul $A[X]$).

Propoziția 2.3. *Relația de divizibilitate pe $A[X]$ are proprietățile :*

1) *$f|f$, oricare ar fi $f \in A[X]$;*

2) *dacă $f|g$ și $g|h$, atunci $f|h$, oricare ar fi f, g, $h \in A[X]$;*

3) *dacă $f|g_1$ și $f|g_2$, atunci $f|g_1h_1 + g_2h_2$, oricare ar fi h_1, h_2 din $A[X]$.*

Demonstrația acestei propoziții este imediată.

Amintim (vezi propoziția 1.3) că elementele inversabile din $A[X]$ coincid cu elementele inversabile din A.

Fie f, $g \in A[X]$. Spunem că f este *asociat în divizibilitate* cu g și scriem $f \sim g$ dacă $f|g$ și $g|f$ în inelul $A[X]$.

Relația de asociere în divizibilitate este evident o relație de echivalență (vezi § 3, cap. II), adică este reflexivă, simetrică și tranzitivă.

Propoziția 2.4. *Fie A un domeniu de integritate și $A[X]$ inelul polinoamelor peste A. Dacă f, g sînt două polinoame din $A[X]$, atunci $f \sim g$ dacă și numai dacă există $a \in A$, a inversabil, astfel încît $f = ag$.*

Demonstrație. Presupunem $f \neq 0$ și $g \sim f$. Cum $f|g$ și $g|f$, rezultă $g = fh_1$ și $f = gh_2$ cu h_1, $h_2 \in A[X]$. Așadar, $f = fh_1h_2$, adică $f(1 - h_1h_2) = 0$. Cum $f \neq 0$ și inelul $A[X]$ este domeniu de integritate, rezultă $1 - h_1h_2 = 0$ sau $h_1h_2 = 1$. Deci h_1, h_2 sînt inversabile în $A[X]$ și conform propoziției 1.3 rezultă că h_1, h_2 sînt elemente din A inversabile. Deci, $f = gh_2$ cu $h_2 \in A$ inversabil. Reciproc, fie $f = ag$ cu $a \in A$ inversabil. Atunci $g = bf$, unde $b \in A$ este inversul lui a și deci $g|f$ și $f|g$, de unde $f \sim g$. Dacă $f = 0$, atunci și $g = 0$ și afirmația din enunț este evidentă.

Definiția 2.1. Fie A un domeniu de integritate și f, g două polinoame din $A[X]$. Un polinom $d \in A[X]$ se numește *cel*

mai mare divizor comun (*c.m.m.d.c.*) al lui f şi g dacă sînt îndeplinite condiţiile:

1° $d|f$ şi $d|g$;

2° dacă $h \in A[X]$ iar $h|f$ şi $h|g$, atunci $h|d$.

Dacă d' este un alt polinom din $A[X]$ care verifică 1° şi 2°, rezultă că $d|d'$ şi $d'|d$, deci $d \sim d'$. După propoziţia precedentă, avem că există $a \in A$ inversabil cu $d' = ad$. Aşadar, cel mai mare divizor comun a două polinoame din $A[X]$, în cazul că există, este unic, mai puţin o asociere în divizibilitate. În general, se alege unul dintre aceştia ca fiind cel mai mare divizor comun al polinoamelor f şi g şi se notează prin (f, g).

Fie K un corp comutativ. Printre polinoamele asociate în divizibilitate cu un polinom dat există unul singur care este unitar, adică are coeficientul termenului de grad maxim egal cu 1. În acest caz, f şi g fiind două polinoame din $K[X]$, vom nota prin (f, g) acel polinom unitar care este un cel mai mare divizor comun al lor. Cum pentru $f = g = 0$ polinomul (f, g) nu poate fi definit ca mai sus, convenim să punem în acest caz $(0, 0) = 0$.

Vom arăta în continuare că orice două polinoame din inelul $K[X]$ (K fiind un corp comutativ) au un cel mai mare divizor comun. Dacă $f|g$, atunci $(f, g) = f$; în particular, $(f, 0) = f$.

Teorema 2.5. *Fie $K[X]$ inelul polinoamelor cu coeficienţi într-un corp comutativ K. Pentru orice două polinoame f, g din $K[X]$ există cel mai mare divizor comun al lor. Mai mult, dacă $d = (f, g)$, atunci există polinoamele h_1, $h_2 \in K[X]$ astfel încît*

$$d = fh_1 + gh_2.$$

Demonstraţie. Dacă $f = g = 0$, teorema este evidentă. Fie $f \neq 0$ sau măcar $g \neq 0$ şi fie

$$I = \{fu + gv \mid u, v \in A[X]\}.$$

Dacă $h|f$ şi $h|g$, conform propoziţiei 2.3, 3), rezultă că $h|fu + gv$, oricare ar fi u, v din $A[X]$. Deci orice divizor al lui f şi g divide orice element din I. Întrucît $f = f \cdot 1 + g \cdot 0$ şi $g = f \cdot 0 + g \cdot 1$, rezultă că $f, g \in A[X]$. Deci I conţine elemente nenule. Atunci mulţimea

$$D_{f,g} = \{\text{grad}\,(h) \mid h \in I,\ h \neq 0\}$$

este o submulţime nevidă de numere naturale.

Fie $d = fh_1 + gh_2 \in I$ astfel încît grad (d) să fie cel mai mic număr natural din $D_{f,g}$. Să arătăm că $d = (f, g)$. Deoarece $d \in I$, orice divizor al lui f şi g divide pe d, deci este verificată, condiţia 2° din definiţia 2.1. Să probăm că d are şi proprietatea 1° a aceleiaşi definiţii. Cum $d \neq 0$, după teorema 2.1 există q, $r \in A[X]$ astfel încît

$$f = dq + r \text{ şi } \operatorname{grad}(r) < \operatorname{grad}(d).$$

Avem

$$r = f - dq = f - (fh_1 + gh_2)q = f(1 - h_1q) + g(-h_2q) \in I.$$

Întrucît $d \in I$ şi este astfel încît grad (d) să fie minim în $D_{f,g}$ iar grad $(r) <$ grad (d), rezultă în mod necesar $r = 0$. Aşadar, $f = dq$ şi deci $d|f$. Analog, se arată că $d|g$. Deci $d = (f, g)$ şi din demonstraţie avem că

$$d = fh_1 + gh_2 \text{ cu } h_1, h_2 \in A[X].$$

Definiţia 2.2. Două polinoame f şi g din $K[X]$ se numesc *prime* între ele (sau relativ prime), dacă $(f, g) = 1$.

Avem că f şi g sînt prime între ele dacă şi numai dacă există h_1 şi h_2 din $A[X]$:

$$fh_1 + gh_2 = 1.$$

Observaţie. Există o metodă constructivă de calcul a celui mai mare divizor comun a două polinoame cunoscută sub numele de algoritmul lui Euclid. Noi nu ne oprim asupra ei.

§ 3. Rădăcinile unui polinom. Proprietăţi

Fie A un inel şi f un polinom din $A[X]$. În § 1 am definit o rădăcină sau un zero al polinomului f. Astfel, $x \in A$ este o rădăcină a lui f dacă $f(x) = 0$.

Propoziţia 3.1. *Fie A un domeniu de integritate, f un polinom din $A[X]$ şi x un element din A. Atunci există un unic polinom g din $A[X]$ astfel încît*

$$f = (X - x)g + f(x).$$

Demonstrație. Din teorema 2.1 rezultă că există q și r din $A[X]$, unice, astfel încît

$$f = (X - x)q + r, \text{ unde grad } (r) < \text{grad } (X - x).$$

Deci $r \in A$ și dacă facem $X = x$, rezultă $r = f(x)$. Așadar,

$$f = (X - x)q + f(x).$$

În particular, rezultă de aici

Corolarul 3.2. *Un polinom $f \in A[X]$ (A domeniu de integritate) este divizibil prin $X - x$ ($x \in A$) dacă și numai dacă x este o rădăcină a lui f.*

Acest corolar este important, deoarece ne spune că rădăcinile unui polinom corespund factorilor săi de gradul întîi.

Fie A un domeniu de integritate, f un polinom din $A[X]$ și $x \in A$. Dacă $(X - x)^s$ $(s \geqslant 1)$ divide pe f în $A[X]$, atunci există un polinom g din $A[X]$ astfel încît

$$f = (X - x)^s g.$$

$(X-x)^s$ fiind polinom unitar, rezultă că g este unic determinat și avem

$$\text{grad } g = \text{grad } f - s.$$

Definiția 3.1. Se spune că un element x din domeniul de integritate A este *rădăcină multiplă de ordinul k* sau *rădăcină de ordinul de multiplicitate k* a polinomului f din $A[X]$ dacă $(X - x)^k$ divide pe f iar $(X - x)^{k+1}$ nu divide pe f.

Este clar că x din A este rădăcină multiplă de ordinul k a lui f dacă și numai dacă există un polinom g din $A[X]$ astfel încît

$$f = (X - x)^k g \text{ cu } g(x) \neq 0.$$

Numărul k există întotdeauna și se numește *ordinul de multiplicitate* al rădăcinii a a lui f.

Observație. Dacă A este un domeniu de integritate iar $x \in A$ este o rădăcină multiplă de ordinul k, respectiv 1, a polinomului f, respectiv g, atunci x este o rădăcină multiplă de ordinul $k + 1$ a produsului fg.

Într-adevăr, avem

$$f = (X - x)^k f_1,\ g = (X - x)^1 g_1,$$

cu $f_1, g_1 \in A[X]$ şi $f_1(x) \neq 0$, $g_1(x) \neq 0$. Deci

$$fg = (X - x)^{k+1} f_1 g_1$$

şi $f_1(x)\, g_1(x) \neq 0$, A fiind domeniu de integritate.

Propoziţia 3.3. *Fie A un domeniu de integritate şi f un polinom nenul din $A[X]$. Dacă $x_1, x_2, \ldots, x_n$ din A sînt rădăcini distincte ale lui f, avînd ordinele de multiplicitate $k_1, k_2, \ldots$ $\ldots, k_n$, atunci f se scrie sub forma*

$$f = (X - x_1)^{k_1}(X - x_2)^{k_2} \ldots (X - x_n)^{k_n} g,$$

unde $g \in A[X]$.

Demonstraţie. Demonstrăm prin inducţie după n. Pentru $n = 1$, propoziţia rezultă din definiţia 3.1. Presupunem că ea este adevărată pentru $n - 1$ şi să demonstrăm pentru n. Există $f_1 \in A[X]$ astfel încît

$$f = (X - x_1)^{k_1} \ldots (X - x_{n-1})^{k_{n-1}} f_1.$$

Dacă $X = x_n$, atunci

$$f(x_n) = (x_n - x_1)^{k_1} \ldots (x_n - x_{n-1})^{k_{n-1}} f_1(x_n) = 0.$$

Dar $x_n \neq x_i$ pentru $i = 1, 2, \ldots, n - 1$ şi cum A este domeniu de integritate, rezultă $f_1(x_n) = 0$. Deoarece a_n nu este rădăcină a polinomului

$$h = (X - x_1)^{k_1} \ldots (X - x_{n-1})^{k_{n-1}},$$

atunci a_n este rădăcină multiplă de ordin k_n a lui f_1 şi deci $f_1 = (X - x_n)^{k_n} g$ cu $g \in A[X]$ şi totul este demonstrat.

Observaţie. Cînd numărăm rădăcinile unui polinom şi nu specificăm că sînt distincte, luăm fiecare rădăcină de atîtea ori cît este ordinul său de multiplicitate.

De mai sus, rezultă evident:

Corolarul 3.4. *Fie A un domeniu de integritate şi f un polinom din $A[X]$ de grad $n > 0$. Atunci f are cel mult n rădăcini în A.*

Corolarul 3.5. *Fie A un domeniu de integritate şi f un polinom nenul din $A[X]$ de grad n. Dacă*

$$f = a_0 + a_1X + \ldots + a_nX^n$$

şi $x_1, x_2, \ldots, x_n$ sînt n rădăcini ale lui f în A, atunci

$$f = a_n(X - x_1)(X - x_2)\ldots(X - x_n)$$

şi

$$-a_{n-1} = a_n(x_1 + x_2 + \ldots + x_n),$$

$$a_{n-2} = a_n(x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n) = a_n \sum_{1 \leqslant i < j \leqslant n} x_ix_j,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(-1)^n a_0 = a_n\, x_1x_2\ldots x_n.$$

Demonstraţie. Din propoziţia 3.3 putem să scriem $f = (X - x_1)(X - x_2)\ldots(X - x_n)g$. Se observă imediat că grad $g = 0$ şi deci $g \in A$. Cum coeficientul termenului de grad maxim al polinomului $(X - x_1)(X - x_2)\ldots(X - x_n)$ este egal cu 1, atunci $g = a_n$. Pe de altă parte putem scrie

$$a_n(X - x_1)(X - x_2)\ldots(X - x_n) = a_nX^n - a_n(x_1 + x_2 + \ldots$$

$$\ldots + x_n)X^{n-1} + a_n(x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n)X^{n-2} + \ldots$$

$$\ldots + (-1)^n a_nx_1x_2\ldots x_n.$$

Identificînd coeficienţii în cele două scrieri ale lui f, se obţin relaţiile cerute. Relaţiile din corolarul precedent se numesc *relaţiile dintre rădăcini şi coeficienţi* (sau *relaţiile lui Viète*).

Corolarul 3.6 (*teorema lui Wilson*). *Dacă $p \geqslant 2$ este un număr întreg prim, atunci*

$$(p - 1)! + 1 \equiv 0 \ (mod\ p).$$

Demonstrație. Fie corpul $\mathbb{Z}_p$ și polinomul $X^{p-1} - \hat{1} \in \mathbb{Z}_p[X]$. Cum pentru orice $\hat{x} \in \mathbb{Z}_p$, $\hat{x}^{p-1} = \hat{1}$, rezultă că rădăcinile polinomului $X^{p-1} - \hat{1}$ sînt $\hat{1}, \hat{2}, \ldots, \widehat{p-1}$. Avînd în vedere corolarul precedent, avem

$$\hat{1} \cdot \hat{2} \cdot \ldots \cdot \widehat{p-1} = -\hat{1}$$

sau $\widehat{(p-1)!} = -\hat{1}$, adică $(p-1)! \equiv -1 \pmod{p}$, de unde

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Vom da în continuare un criteriu de existență a rădăcinilor multiple ale unui polinom. Pentru aceasta vom spune ce înseamnă derivata unui polinom cu coeficienți într-un corp comutativ K. Să considerăm aplicația

$$\mathrm{d} : K[X] \to K[X]$$

definită în modul următor : dacă $a \in K$, atunci $\mathrm{d}a = 0$ iar dacă $f = \sum_{i=0}^{n} a_i X^i$ este un polinom de grad $\geqslant 1$, atunci $\mathrm{d}f = \sum_{i=1}^{n} i a_i X^{i-1}$.

În particular, $\mathrm{d}X^i = iX^{i-1}$, dacă $i \geqslant 1$, de unde

$$\mathrm{d}X^{i+j} = (i+j)\, X^{i+j-1} = iX^j X^{i-1} + jX^i X^{j-1} = X^j\, \mathrm{d}X^i + X^i\, \mathrm{d}X^j.$$

Așadar, pentru orice f, $g \in K[X]$, avem

$$\mathrm{d}(fg) = g\, \mathrm{d}f + f\, \mathrm{d}g.$$

Mai mult, este clar că d are și proprietățile :

$$\mathrm{d}(f + g) = \mathrm{d}f + \mathrm{d}g \text{ pentru orice } f,\ g \in K[X]$$

și

$$\mathrm{d}(af) = a\mathrm{d}f \text{ pentru orice } a \in A \text{ și } f \in K[X].$$

Definiția 3.2. Pentru $f \in K[X]$, $\mathrm{d}f$ se numește *derivata* polinomului f și se mai notează cu f' sau $f^{(1)}$.

Prin recurență se definește $f^{(n)} = \mathrm{d}^n f = \mathrm{d}(\mathrm{d}^{n-1} f)$ pentru orice număr întreg $n > 1$ și se numește *derivata de ordin n* a lui f. Pentru $n = 0$ se notează $\mathrm{d}^0 f = f^{(0)} = f$.

Lema 3.7. *Fie K un corp comutativ și f din K[X] un polinom nenul de grad n. Dacă $x \in K$ este un element oarecare, atunci f se poate scrie sub forma*

$$f = \sum_{i=0}^{n} b_i (X - x)^i.$$

Demonstrație. Vom demonstra prin inducție, după gradul lui f. Pentru $n = 1$ relația este evidentă. Fie $n > 1$; atunci după propoziția 3.1 rezultă că există $g \in K[X]$ și $b_0 \in K$ astfel încît

$$f = (X - x)\, g + b_0.$$

Deoarece grad $g = n - 1 < n$, din ipoteza inducției, g se scrie în mod unic sub forma

$$g = \sum_{i=0}^{n-1} c_i (X - x)^i,$$

de unde rezultă

$$f = (X - x) \sum_{j=0}^{n-1} c_i (X - x)^i + b_0 = \sum_{i=0}^{n-1} c_i (X - x)^{i+1} + b_0.$$

Dacă punem $c_i = b_{i+1}$, se obține

$$f = \sum_{i=0}^{n} b_i (X - x)^i.$$

De aici rezultă că pentru orice număr i, $1 \leqslant i \leqslant n$, avem

$$f^{(i)}(x) = i\,!\, b_i.$$

Propoziția 3.8. *Fie K un corp, f un polinom nenul din K[X] și $r \geqslant 1$ un număr întreg.*

1) *Dacă $x \in K$ este o rădăcină multiplă de ordin r, atunci $f^{(i)}(x) = 0$, pentru orice $i = 0, 1, 2, \ldots, r - 1$.*

2) *Dacă K este de caracteristică zero şi $f^{(i)}(x) = 0$, pentru $i = 0, 1, 2, \ldots, r-1$, iar $f^{(r)}(x) \neq 0$, atunci x este rădăcină multiplă de ordin r a lui f.*

Demonstraţie. După lema precedentă f se scrie sub forma

$$f = \sum_{i=0}^{n} b_i(X - x)^i,$$

unde $n = \text{grad}(f)$.

1) Dacă x este rădăcină multiplă de ordin r a lui f, atunci $b_i = 0$, $i = 0, 1, 2, \ldots, r-1$, şi cum $f^{(i)}(x) = i!b_i$ $(1 \leqslant i \leqslant n)$, rezultă $f^{(i)}(x) = 0$ pentru $i = 0, 1, 2, \ldots, r-1$.

2) Dacă K este de caracteristică zero şi $f^{(i)}(x) = 0$, pentru $i = 0, 1, 2, \ldots, r-1$, atunci din lema precedentă rezultă $b_i = 0$, pentru $i = 0, 1, 2, \ldots, r-1$. Deci x este o rădăcină multiplă de ordin r şi nu este de ordin $> r$, deoarece atunci ar trebui ca $f^r(x) = 0$.

Observaţie. Afirmaţia 2) a propoziţiei precedente nu este adevărată pentru corpurile de caracteristică nenulă. Într-adevăr, fie, de exemplu, corpul $\mathbb{Z}_p$, cu p prim şi polinomul $f = X^p$. Avem că f are pe 0 ca rădăcină multiplă de ordin p, dar $f^{(i)}(0) = 0$, pentru orice $i > 0$.

§ 4. Polinoame ireductibile în inele de polinoame cu coeficienţi într-un corp. Descompunerea polinoamelor în factori ireductibili

Fie K un corp comutativ şi $K[X]$ inelul polinoamelor de o nedeterminată cu coeficienţi în K. Polinoamele inversabile din $K[X]$ coincid (v. propoziţia 1.3.) cu elementele nenule din K.

Definiţia 4.1. Un polinom p nenul şi neinversabil se numeşte *ireductibil* dacă din $f|p$ rezultă $f \sim 1$ sau $f \sim p$.

Cu alte cuvinte, un polinom p nenul şi neinversabil este ireductibil dacă singurii divizori ai săi sînt polinoamele inversabile şi cele asociate în divizibilitate cu p (adică cele care diferă de p prin constante nenule) sau, încă, dacă p nu poate fi reprezentat ca produs de două polinoame din $K[X]$, ambele cu gradul strict mai mic decît grad (p).

Un polinom nenul şi neinversabil care nu este ireductibil se numeşte *reductibil.*

Definiţia 4.2. Un polinom q nenul şi neinversabil din $K[X]$ se numeşte *prim* dacă, oricare ar fi f, g din $K[X]$, din $q|fg$ rezultă $q|f$ sau $q|g$.

Propoziţia 4.1. *Un polinom din inelul* $K[X]$ *este ireductibil dacă şi numai dacă este prim.*

Demonstraţie. Fie p un polinom ireductibil şi $p|fg$, $f, g \in K[X]$. Cum p este ireductibil, acesta nu are divizori decît polinoamele inversabile sau cele asociate cu p. Deci, $(p, f) \sim p$ sau $(p, f) = 1$. În primul caz, rezultă $p|f$. Dacă însă $(p, f) = 1$, atunci există h_1, $h_2 \in K[X]$ astfel încît $ph_1 + fh_2 = 1$, de unde, multiplicînd cu g, avem $g = pgh_1 + fgh_2$. Or, cum $p|fg$, rezultă $p|pgh_1 + fgh_2$, deci $p|g$. Reciproc, fie q un polinom prim şi f un divizor al său, adică $q = fg$ cu $f, g \in K[X]$. Cum q este prim şi $q|fg$, rezultă $q|f$ sau $q|g$. Dacă $q|f$ şi cum $f|q$, rezultă $f \sim q$. Dacă însă $q|g$ şi cum $g|q$, avem $g \sim q$ şi deci $f \sim 1$. Aşadar, q este ireductibil.

Teorema 4.2. *Orice polinom nenul şi neinversabil din* $K[X]$ *este produsul unui număr finit de polinoame ireductibile. Mai mult, dacă* $f \in K[X]$ *cu grad* $(f) \geqslant 1$ *şi*

$$f = p_1p_2 \ldots p_m = p'_1p'_2 \ldots p'_n,$$

unde p_i *şi* p'_j *sînt polinoame ireductibile în* $K[X]$, *atunci* $m = n$ *şi există o permutare* $\sigma \in \sigma_n$ astfel încît

$$p_i \sim p'_{\sigma(i)}, \ i = 1, 2, \ldots, n.$$

Demonstraţie. Să demonstrăm mai întîi prima parte a teoremei. Fie pentru aceasta $f \in K[X]$. Dacă f este ireductibil, atunci totul este evident. Dacă nu, adică f este reductibil, există g, $h \in K[X]$ astfel încît $f = gh$, $1 \leqslant$ grad (g), grad $(h) <$ grad (f). În acest caz, vom demonstra prin inducţie după grad.

Presupunînd adevărată proprietatea pentru toate polinoamele de grad mai mic ca cel al lui f, polinoamele g şi h se descompun în produs finit de polinoame ireductibile şi deci $f = gh$

se descompune. Rămîne să demonstrăm partea a doua a teoremei. Demonstrăm prin inducţie după m. Dacă $m = 1$, atunci $f = p_1$ şi deci $n = 1$ şi $p_1' = p_1$. Să presupunem proprietatea adevărată pentru polinoamele ce se descompun în $m - 1$ factori şi să demonstrăm pentru f. Cum p_1 este prim (vezi propoziţia 4.1) şi $p_1 | p_1'p_2' \ldots p_n'$, rezultă că există i astfel încît $p_1 | p_i'$. Renumerotînd termenii, dacă este necesar, putem presupune că $p_1 | p_1'$. Cum p_1' este ireductibil, rezultă $p_1 \sim p_1'$ şi deci $p_1' = p_1\alpha_1$, cu $\alpha \in K$, $\alpha \neq 0$. Din $p_1p_2 \ldots p_m = p_1'p_2' \ldots p_n'$ obţinem

$$p_1p_2 \ldots p_m = \alpha_1 p_1 p_2' \ldots p_n'$$

şi deci

$$p_2p_3 \ldots p_m = p_2''p_3'' \ldots p_n'',$$

unde $p_2'' = \alpha_1 p_2'$ şi $p_j'' = p_j'$ sînt ireductibili. Din ipoteza inducţiei $m - 1 = n - 1$ şi după o eventuală renumerotare a termenilor $p_j \sim p_j''$. Deci $m = n$ şi $p_i \sim p_i'$, $1 \leqslant i \leqslant n$, după o eventuală renumerotare a factorilor. Dar a face o renumerotare a factorilor revine la o aplica o permutare indicilor acestora, aşa că totul este demonstrat.

Fie f un polinom din $K[X]$ şi

$$(f) = fK[X] = \{g | g \in K[X], f | g\}.$$

(f) este un ideal al lui $K[X]$, numit *idealul principal* generat de f.

Fie inelul factor $K[X]/(f)$ şi $\alpha \in K[X]/(f)$ un element al său. Atunci α este clasa unui polinom $g \in K[X]$, adică $\alpha = \hat{g}$. Scriem teorema împărţirii cu rest între g şi f şi obţinem

$$g = fq + r, \text{ unde grad } (r) < \text{grad } (f).$$

Deci $\alpha = \hat{g} = \widehat{fq + r} = \widehat{fq} + \hat{r} = \hat{r}$. Aşadar, orice element din inelul factor $K[X]/(f)$ este clasa unui polinom de grad strict mai mic decît gradul lui f.

Definim $\varphi : K \to K[X]/(f)$ prin

$$\varphi(x) = \hat{x},$$

care este evident un omomorfism injectiv de inele. Astfel, l poate fi privit ca un subcorp al lui $K[X]/(f)$ identificînd $x =$ sau, cum se mai spune, $K[X]/(f)$ este o extindere a lui K.

Lema 4.3. *Dacă $f \in K[X]$ este un polinom ireductibil, atunc $K[X]/(f)$ este un corp.*

Demonstrație. Fie $\alpha \in K[X]/(f)$, $\alpha \neq 0$. Atunci $\alpha = \hat{r}$ cı grad $(r) <$ grad (f). Cum f este ireductibil și grad $(r) <$ grad (f), atunci $(f, r) = 1$. Deci, există $u, v \in K[X]$ astfel încît $fu + rv =$ $= 1$, de unde, trecînd la clase, se obține $\widehat{fu} + \widehat{rv} = \hat{1}$, deci $\hat{r}\hat{v} = 1$, adică $\alpha = \hat{r}$ este inversabil.

Propoziția 4.4. *Fie $f \in K[X]$ un polinom ireductibil. Atunci există o extindere a lui K în care f are o rădăcină.*

Demonstrație. Cum f este ireductibil, conform lemei precedente, $E = K[X]/(f)$ este un corp care este o extindere a lui K. Dacă $f = a_0 + a_1X + \dots + a_nX^n$, atunci $0 = \hat{f}(X) =$ $= \widehat{a_0 + a_1X + \dots + a_nX^n} = a_0 + a_1\hat{X} + \dots + a_n\hat{X}^n = f(\hat{X})$. Deci $\hat{X} \in E$ este o rădăcină a lui f.

Propoziția 4.5. *Fie f un polinom din $K[X]$ de grad $n \geqslant 1$. Atunci există o extindere E a lui K astfel încît f să aibă n rădăcini în E.*

Demonstrație. Din propoziția precedentă, rezultă că pentru un factor ireductibil al lui f există o extindere a lui K în care acesta are o rădăcină, care dealtfel este și rădăcină a lui f. Facem demonstrația prin inducție după n. Pentru $n = 1$ este evident. Fie $n > 1$ și presupunem afirmația adevărată pentru polinoamele de grad $\leqslant n - 1$, cu coeficienți într-un corp. Atunci, pentru polinomul f dat, considerăm un factor ireductibil al său care are o rădăcină (vezi propoziția precedentă) într-o anumită extindere a lui K. Dar aceasta este și rădăcină a lui f și deci am arătat că pentru f există o extindere a lui K în care el să aibă o rădăcină și deci $f = (X - a)g$, $a \in K$ și $g \in K[X]$ de grad $n - 1$. Din ipoteza inductivă rezultă că există o extindere a lui K în care g să aibă $n - 1$ rădăcini. Este clar că în această extindere f nu are rădăcini.

Propoziția 4.6. *Fie K un corp de caracteristică zero și f un polinom ireductibil din $K[X]$. Atunci rădăcinile lui f (care se găsesc într-o extindere E a lui K) sînt distincte.*

Demonstrație. Să presupunem că f are o rădăcină $\alpha \in E$, care este multiplă, adică $f(\alpha) = f'(\alpha) = 0$. Cum f este ireductibil, avem $(f, f') = 1$ și deci există g, $h \in K[X]$ astfel încît $hf + gf' = 1$. Considerăm această relație în $E[X]$ și punem $X = \alpha$. Atunci $0 = 1$, deci am ajuns la o contradicție.

Dăm, în final, un criteriu de ireductibilitate în $\mathbb{Q}[X]$ al polinoamelor cu coeficienți întregi, cunoscut sub denumirea de *criteriul lui Eisenstein.*

Propoziția 4.7 (*Eisenstein*). *Fie $f = a_0 + a_1X + \ldots + a_nX^n$ un polinom de grad $n \geqslant 1$ din $\mathbb{Z}[X]$ și fie p un număr prim. Dacă $a_0 \not\equiv 0 \pmod p$, $a_i \equiv 0 \pmod p$, pentru $1 \leqslant i \leqslant n$, și $a_n \not\equiv 0 \pmod{p^2}$, atunci f este ireductibil în inelul $\mathbb{Q}[X]$.*

Demonstrație. Putem presupune că coeficienții $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ sînt primi între ei, deoarece, în caz contrar, scriem $f = dg$, unde d este cel mai mare divizor comun al coeficienților și vom raționa pentru g. Să presupunem prin absurd că există un număr prim p astfel încît să fie satisfăcute condițiile de enunț, și totuși

$$f = f_1f_2, \text{ cu } \operatorname{grad} f_1, \operatorname{grad} f_2 \geqslant 1,$$

în inelul $\mathbb{Q}[X]$. Atunci polinomul f admite această descompunere în $\mathbb{Z}[X]$. Așadar,

$$f_1 = b_0 + b_1X + \ldots + b_qX^q,$$

$$f_2 = c_0 + c_1X + \ldots + c_mX^m,$$

cu b_i, $c_j \in \mathbb{Z}$, q, $m \geqslant 1$ și b_q, $c_m \neq 0$. Putem scrie deci

$$a_0 + a_1X + \ldots + a_nX^n =$$

$$= (b_0 + b_1X + \ldots + b_qX^q)(c_0 + c_1X + \ldots + c_mX^m)$$

în inelul $\mathbb{Z}[X]$. Reducînd modulo p această egalitate, se obţine în $\mathbb{Z}_p[X]$ descompunerea

$$\hat{a}_0 + \hat{a}_1 X + \ldots + \hat{a}_n X^n =$$

$$= (\hat{b}_0 + \hat{b}_1 X + \ldots + \hat{b}_q X^q)(\hat{c}_0 + \hat{c}_1 X + \ldots + \hat{c}_m X^m)$$

şi deci

$$\hat{a}_n X^n = (\hat{b}_0 + \hat{b}_1 X + \ldots + \hat{b}_q X^q)(\hat{c}_0 + \hat{c}_1 X + \ldots + \hat{c}_m X^m).$$

Cum $\mathbb{Z}_p$ este corp, atunci, după teorema 4.3, descompunerea în factori ireductibili este unică şi deci

$$\hat{a}_m X^n = \hat{b}_q X^q \cdot \hat{c}_m X^m$$

iar $\hat{b}_0 = \hat{c}_0 = \hat{0}$. Deci $b_0 \equiv 0 \pmod p$ şi $c_0 \equiv 0 \pmod p$, de unde $b_0 c_0 \equiv 0 \pmod{p^2}$. Dar, cum $a_0 = b_0 c_0$, se contrazice ipoteza.

Aplicaţii. Fie p un număr prim. Atunci polinomul

$$f = 1 + X + \ldots + X^{p-1}$$

este ireductibil în $\mathbb{Q}[X]$. Într-adevăr, este suficient să dovedim că polinomul $f(X+1)$ este ireductibil în $\mathbb{Q}[X]$. Dar

$$f(X+1) = \frac{(X+1)^p - 1}{X+1-1} = \frac{X^p + C_p^1 X^{p-1} + \ldots + C_p^{p-1} X}{X} =$$

$$= X^{p-1} + C_p^1 X^{p-2} + \ldots + C_p^{p-1}.$$

Deoarece numerele $C_p^k = \dfrac{p!}{k!(p-k)!}$, $1 \leqslant k \leqslant p-1$, sînt multipli de p iar $C_p^{p-1} = p \not\equiv 0 \pmod{p^2}$, conform criteriului lui Eisenstein polinomul $f(X+1)$ este ireductibil în $\mathbb{Q}[X]$. Deci, f este ireductibil în inelul $\mathbb{Q}[X]$.

2) Fie p un număr prim şi $a \in \mathbb{Z}$ astfel încît $(a, p) = 1$. Atunci polinomul $X^p - X + a \in \mathbb{Q}[X]$ este ireductibil.

Criteriul lui Eisenstein nu se poate aplica în acest caz. Vom proceda astfel. Notăm $f = X^p - X + a$ şi presupunem că $f = gh$ cu $g, h \in \mathbb{Q}[X]$ şi grad $g \geqslant 1$, grad $h \geqslant 1$. Cum f are coeficienţii întregi, atunci rezultă că g şi h sînt polinoame cu coeficienţi întregi. În plus, coeficientul termenilor de grad maxim din g şi h este egal cu 1.

Considerăm corpul $\mathbb{Z}_p$. Dacă $P = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{Z}[X]$, notăm $\bar{P} = \hat{a}_0 + \hat{a}_1X + \ldots + \hat{a}_nX^n \in \mathbb{Z}_p[X]$. Din egalitatea $f = gh$ obținem $\bar{f} = \bar{g}\bar{h}$ în $\mathbb{Z}_p[X]$ cu grad $\bar{g} \geqslant 1$ și grad $\bar{h} \geqslant 1$. Dar $\bar{f} = X^p - X + \hat{a}$, $\hat{a} \in \mathbb{Z}_p$, $\hat{a} \neq 0$.

Fie K o extindere a corpului $\mathbb{Z}_p$ unde $\bar{f}$ are p rădăcini; fie α una dintre aceste rădăcini. Deci, $\alpha^p - \alpha + \hat{a} = 0$. Din teorema lui Fermat rezultă că $\alpha \notin \mathbb{Z}_p$. Dacă $\hat{b} \in \mathbb{Z}_p$, atunci din egalitatea

$$(\alpha + \hat{b})^p = \alpha^p + C_p^1\alpha^{p-1}\hat{b} + C_p^2\alpha^{p-2}\hat{b}^2 + \ldots + \hat{b}^p$$

și din faptul că $p \mid C_p^k$, $1 \leqslant k \leqslant p - 1$, obținem

$$(\alpha + \hat{b})^p = \alpha^p + \hat{b}^p.$$

Calculăm

$$(\alpha + \hat{b}) = (\alpha + \hat{b})^p - (\alpha + \hat{b}) + \hat{a} = \alpha^p + \hat{b}^p - \alpha - \hat{b} + \hat{a} =$$

$$= (\alpha^p - \alpha + \hat{a}) + (\hat{b}^p - \hat{b}) = \hat{b}^p - \hat{b}.$$

Folosind teorema lui Fermat, deducem că

$$\hat{b}^p - \hat{b} = 0.$$

Deci $\bar{f}(\alpha + \hat{b}) = 0$ și, prin urmare, $\alpha + \hat{b}$ este de asemenea o rădăcină a lui $\bar{f}$. Deci rădăcinile lui $\bar{f}$ în corpul K sînt α, $\alpha + \hat{1}$, $\alpha + \hat{2}$, $\ldots$, $\alpha + \widehat{(p - 1)}$. Astfel, $\bar{f}$ are în $K[X]$ următoarea descompunere:

$$\bar{f} = (X - \alpha)(X - \alpha - \hat{1}) \ldots (X - \alpha - \widehat{p - 1}).$$

Deoarece $\bar{f} = \bar{g}\bar{h}$, atunci $\bar{g}$ este de forma

$$\bar{g} = (X - \alpha - \hat{i}_1)(X - \alpha - \hat{i}_2) \ldots (X - \alpha - \hat{i}_k), \text{ unde } 1 \leqslant k \leqslant p - 1.$$

Cum $\bar{g} \in \mathbb{Z}_p[X]$, atunci

$$k\alpha + \sum_{j=1}^{k} \hat{i}_j \in \mathbb{Z}_p$$

și deci $k\alpha \in \mathbb{Z}_p$. Avînd în vedere că $1 \leqslant k \leqslant p - 1$, obținem $\alpha \in \mathbb{Z}_p$, ceea ce este în contradicție cu $\alpha \notin \mathbb{Z}_p$.

§ 5. Inelul polinoamelor de mai multe nedeterminate

Definim la început, prin inducție, inelul polinoamelor de un număr finit de nedeterminate.

Fie A un inel. Atunci inelul $A[X_1, X_2, \ldots, X_n]$ al polinoamelor în nedeterminatele $X_1, X_2, \ldots, X_n$ cu coeficienți în inelul A se definește, inductiv, astfel : $A[X_1]$ este inelul polinoamelor în nedeterminata X_1 cu coeficienți în inelul A și, în general, $A[X_1, X_2, \ldots, X_i]$ este inelul polinoamelor în nedeterminata X_i cu coeficienți în inelul $A[X_1, X_2, \ldots, X_{i-1}]$, $1 \leqslant i \leqslant n$. Deci

$$A[X_1, X_2, \ldots, X_n] = A[X_1, X_2, \ldots, X_{n-1}]\,[X_n].$$

Dacă f este un polinom din $A[X_1, X_2, \ldots, X_n]$, atunci f este un polinom în nedeterminata X_n cu coeficienți în $A[X_1, X_2, \ldots$ $\ldots, X_{n-1}]$. Așadar,

$$f = f_0 + f_1X_n + \ldots + f_kX_n^k, \quad \text{unde } f_i \in A[X_1, X_2, \ldots, X_{n-1}],$$

oricare ar fi $i = 0, 1, \ldots, k$. Este clar că, din aproape în aproape, f se poate scrie ca o sumă finită de forma $\sum a_{i_1i_2\ldots i_n}X_1^{i_1}X_2^{i_2}\ldots X_n^{i_n}$, în care $a_{i_1i_2\ldots i_n} \in A$ se numesc *coeficienții* polinomului f. Deci

$$f = \sum_{i_1, i_2, \ldots, i_n = 0}^{k_1, k_2, \ldots, k_n} a_{i_1i_2\ldots i_n}X_1^{i_1}X_2^{i_2}\ldots X_n^{i_n}$$

unde $k_1, k_2, \ldots, k_n$ sînt numere naturale.

Să arătăm că o astfel de scriere este unică. Într-adevăr, dacă $f = 0$, din definiție, rezultă că f poate fi scris sub forma

$$f = \sum_{i=0}^{k_n} f_iX_n^i,$$

unde f_i sînt polinoame din $A[X_1, X_2, \ldots, X_{n-1}]$. Observăm de asemenea că orice coeficient $a_{i_1i_2\ldots i_n}$ apare drept coeficient al unuia din polinoamele f_i. Atunci fiecare $f_i = 0$ și deci, prin inducție, rezultă că toți coeficienții $a_{i_1i_2\ldots i_n}$ sînt nuli. De aici rezultă unicitatea scrierii lui f sub forma indicată.

Fiind dat inelul de polinoame $A[X_1, X_2, \ldots, X_n]$ cu coeficienți într-un inel A și f un polinom din acest inel, gradul lui f relativ la nedeterminata X_i, $i = 1, 2, \ldots, n$, este cel mai mare exponent la care figurează X_i în expresia lui f. Se poate întîmpla ca acest grad să fie 0, ceea ce înseamnă că nedeterminata X_i nu intervine în expresia lui f. Un polinom de forma $aX_1^{k_1}X_2^{k_2} \ldots X_n^{k_n}$ cu $a \neq 0$ se numește *monom* iar prin gradul său înțelegem suma $k_1 + k_2 + \ldots + k_n$, adică suma exponenților nedeterminatelor. Cum orice polinom f este o sumă finită de monoame, vom defini gradul lui f ca fiind maximul gradelor termenilor săi și îl vom nota cu grad (f).

Dacă toți termenii (monoamele) unui polinom au același grad, atunci f se numește *polinom omogen* sau *formă*. Dacă f și g sînt două forme, atunci sau fg va fi polinomul nul, sau o formă nenulă de grad egal cu grad (f) + grad (g).

Polinomul $f \neq 0$, de grad n, se poate scrie în mod unic sub forma

$$f = f_0 + f_1 + \cdots + f_n,$$

unde fiecare f_i este nul, sau dacă nu, este o formă de grad i și $f_n \neq 0$. De aici rezultă că dacă $f, g \in A[X_1, X_2, \ldots, X_n]$, atunci

$$\text{grad}\,(fg) \leqslant \text{grad}\,(f) + \text{grad}\,(g).$$

De asemenea, este evident că

$$\text{grad}\,(f + g) \leqslant \text{grad}\,(f) + \text{grad}\,(g).$$

Propoziția 5.1. *Dacă A este un domeniu de integritate, atunci $A[X_1, X_2, \ldots, X_n]$ este domeniu de integritate și, oricare ar fi două polinoame f, g, avem*

$$\textit{grad}\,(fg) = \textit{grad}\,(f) + \textit{grad}\,(g).$$

Demonstrație. Să demonstrăm, prin inducție după n, că $A[X_1, X_2, \ldots, X_n]$ este domeniu de integritate. Într-adevăr, pentru $n = 1$ s-a demonstrat în §1 și apoi se are în vedere că

$$A[X_1, X_2, \ldots, X_n] = A[X_1, X_2, \ldots, X_{n-1}]\,[X_n].$$

Presupunem că f şi g sînt polinoame nenule de grade p şi q respectiv. Scriem

$$f = f_0 + f_1 + \ldots + f_p,\ g = g_0 + g_1 + \ldots + g_q,\ f_p \neq 0,\ g_q \neq 0$$

unde f_i, g_j sînt sau egale cu zero, sau forme de grad i şi j respectiv. Apoi

$$fg = \sum_{k=0}^{p+q} h_k,\ h_k = \sum_{i+j=k} f_i g_j.$$

Deoarece $A[X_1, X_2, \ldots, X_n]$ este domeniu de integritate, $h_{p+q} = f_p g_q \neq 0$ şi rezultă relaţia cerută.

În general, un polinom de mai multe nedeterminate poate avea mai mulţi termeni de grad maxim (în sensul definit mai sus) şi, astfel, nu putem vorbi de un termen bine individualizat.

Pentru polinoamele de mai multe nedeterminate există un mod bine definit de a ordona termenii unui polinom care, în particular, pentru polinoamele de o nedeterminată ne dă scrierea după puterile descrescătoare ale nedeterminatei. Acest mod de a ordona termenii, zis lexicografic, este sugerat de metoda uzuală de a ordona cuvintele într-un dicţionar. Dacă literele sînt ordonate urmînd ordinea alfabetică, se defineşte locul cuvintelor într-un dicţionar prin prima literă iar dacă două cuvinte au primele litere aceleaşi, se defineşte locul lor prin literele care urmează imediat primelor litere etc.

Fie două monoame $M_1 = aX_1^{i_1}X_2^{i_2}\ldots X_n^{i_n}$ şi $M_2 = bX_1^{j_1}X_2^{j_2}\ldots X_n^{j_n}$ din $A[X_1, X_2, \ldots, X_n]$. Se spune că M_1 este *mai mare* (*în ordine lexicografică*) decît M_2 şi scriem $M_1 > M_2$ dacă există un număr natural s, $1 \leqslant s \leqslant n$, astfel încît $i_1 = j_1$, $i_2 = j_2, \ldots, i_{s-1} = j_{s-1}$, $i_s > j_s$. Cum un polinom se scrie în mod unic, ca sumă de monoame diferite între ele, rezultă că, utilizînd ordonarea lexicografică, putem vorbi de un termen al său (monom) cu coeficient nenul bine determinat care să fie cel mai mare în ordinea lexicografică. Acesta se numeşte *termenul principal* al polinomului.

Lema 5.2. *Fie M_1, M_2 două monoame din $A[X_1, X_2, \ldots, X_n]$ astfel încît $M_1 > M_2$. Atunci:*

1) *Oricare ar fi monomul N astfel încît produsele coeficientului său cu coeficienţii lui M_1 şi respectiv M_2 să nu fie nule, rezultă $M_1N > M_2N$.*

2) *Oricare ar fi monoamele* N_1, N_2 *astfel încît produsul coeficienților lui* M_i *și* N_i, *pentru* $i = 1, 2$, *să nu fie nul și dacă* $N_1 > N_2$, *rezultă* $M_1N_1 > M_2N_2$.

Demonstrație. 1) Dacă $M_1 = aX_1^{u_1}X_2^{u_2} \dots X_n^{u_n}$ și $M_2 = bX_1^{v_1}X_2^{v_2} \dots X_n^{v_n}$ și dacă $M_1 > M_2$, atunci fie $u_1 = v_1$, $u_2 = v_2, \dots, u_{i-1} = v_{i-1}$, $u_i > v_i$. Dacă $N = cX_1^{w_1}X_2^{w_2} \dots X_n^{w_n}$ este un monom oarecare, atunci

$$u_1 + w_1 = v_1 + w_1,\ u_2 + w_2 = v_2 + w_2, \dots, u_{i-1} + w_{i-1} =$$

$$= v_{i-1} + w_{i-1},\ u_i + w_i > v_i + w_i,$$

ceea ce demonstrează 1).

2) Dacă acum $N_1 > N_2$, atunci conform cu 1), rezultă $M_1N_1 > M_1N_2 > M_2N_2$, deci este demonstrat 2).

Propoziția 5.3. *Termenul principal al produsului a două polinoame este egal cu produsul termenilor principali, dacă produsul coeficienților celor doi termeni nu este nul.*

Demonstrație. Fie f și g două polinoame din $A[X_1, X_2, \dots, X_n]$ și fie $aX_1^{r_1}X_2^{r_2} \dots X_n^{r_n}$ și $bX_1^{s_1}X_2^{s_2} \dots X_n^{s_n}$ termenii principali respectivi, astfel încît $ab \neq 0$. Avem că termenul principal al produsului fg este

$$abX_1^{r_1+s_1}X_2^{r_2+s_2} \dots X_n^{r_n+s_n}.$$

Din lema precedentă rezultă că acest termen care este nenul este mai mare decît oricare alt termen al produsului celor două polinoame, așa că nu se reduce cu nici unul.

§ 6. Polinoame simetrice

Printre polinoamele de mai multe nedeterminate remarcăm pe cele care sînt invariante la orice permutare a nedeterminatelor. Nedeterminatele intervin deci în mod simetric în expresia acestor polinoame, ceea ce determină și denumirea lor de *polinoame simetrice.*

Mai precis, fie σ_n grupul permutărilor de n elemente iar un polinom din $A[X_1, X_2, \ldots, X_n]$ şi anume

$$f = \sum a_{i_1 i_2 \ldots i_n} X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}.$$

Dacă $\sigma \in \sigma_n$ este o permutare de n elemente, atunci se pun

$$\sigma \cdot f = \sum a_{i_1 i_2 \ldots i_n} X_{\sigma(1)}^{i_1} X_{\sigma(2)}^{i_2} \ldots X_{\sigma(n)}^{i_n} = f(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}).$$

Asocierea $f \to \sigma \cdot f$ defineşte un omomorfism de inele

$$\sigma^* : A[X_1, X_2, \ldots, X_n] \to A[X_1, X_2, \ldots, X_n]$$

care este unic cu proprietatea că $\sigma^*(a) = \sigma a = a$, oricare ar fi $a \in A$ şi $\sigma^*(X_i) = \sigma X_i = X_{\sigma(i)}$, pentru $i = 1, 2, \ldots, n$.

Observăm că, au loc relaţiile :

1. Dacă $\sigma, \tau \in \sigma_n$, atunci $(\sigma\tau)f = \sigma(\tau f)$.

2. Dacă e este permutarea identică, atunci $ef = f$, oricare ar fi polinomul $f \in A[X_1, X_2, \ldots, X_n]$.

Omomorfismul σ^* este inversabil, inversul său fiind $(\sigma^{-1})^*$ şi deci σ^* este chiar un izomorfism.

Definiţia 6.1. Un polinom f din $A[X_1, X_2, \ldots, X_n]$ se numeşte *simetric* dacă, pentru orice σ din σ_n, avem $\sigma^*(f) = f$, adică polinomul rămîne invariant la orice permutare a nedeterminatelor sale.

Deoarece orice permutare σ din σ_n se reprezintă ca produs de transpoziţii (vezi corolarul 7.6, cap. II), pentru ca un polinom să fie simetric este necesar şi suficient să fie invariant la toate transpoziţiile din σ_n.

Să notăm cu S mulţimea polinoamelor simetrice de n nedeterminate.

Propoziţia 6.1. *Mulţimea S a polinoamelor simetrice de n nedeterminate formează un subinel al inelului $A[X_1, X_2, \ldots, X_n]$*

Demonstraţie. Într-adevăr, dacă $f, g \in S$, atunci $\sigma^*(f) = f$ şi $\sigma^*(g) = g$, oricare ar fi permutarea $\sigma \in \sigma_n$. Deoarece σ^* este un omomorfism, avem

$$\sigma^*(f - g) = \sigma^*(f) - \sigma^*(g) = f - g \text{ şi } \sigma^*(fg) = \sigma^*(f)\sigma^*(g) = fg$$

Deci $f - g, fg \in S$, adică S este un subinel al inelului $A[X_1, X_2, \ldots, X_n]$.

Considerăm polinomul $g(X) = (X - X_1)(X - X_2)\ldots(X - X_n)$ din $A[X_1, X_2, \ldots, X_n]$. Atunci $g(X) = X^n - s_1 X^{n-1} + \ldots + (-1)^n s_n$, unde elementele $s_i \in A[X_1, X_2, \ldots, X_n]$ au expresiile următoare:

$$s_1 = X_1 + X_2 + \ldots + X_n = \sum_{i=1}^{n} X_i,$$

$$s_2 = X_1X_2 + X_1X_3 + \ldots + X_{n-1}X_n = \sum_{i<j} X_iX_j,$$

$$s_3 = X_1X_2X_3 + X_1X_2X_4 + \ldots + X_{n-2}X_{n-1}X_n = \sum_{i<j<k} X_iX_jX_k,$$

. . . .

$$s_n = X_1X_2\ldots X_n.$$

Propoziția 6.2. *Polinoamele* $s_1, s_2, \ldots, s_n$ *sînt simetrice.*

Demonstrație. Fie $\sigma \in \sigma_n$ o permutare oarecare și omomorfismul $\sigma^* : A[X_1, X_2, \ldots, X_n] \to A[X_1, X_2, \ldots, X_n]$. Considerînd inelul $A[X_1, X_2, \ldots, X_n, X]$ al polinoamelor în nedeterminatele $X_1, X_2, \ldots, X_n, X$ ($n + 1$ nedeterminate) cu coeficienți în A. Fie

$$\sigma^{**} : A[X_1, X_2, \ldots, X_n, X] \to A[X_1, X_2, \ldots, X_n, X]$$

definit astfel: $\sigma^{**}(X_i) = X_{\sigma(i)}$, $1 \leqslant i \leqslant n$, iar $\sigma^{**}(X) = X$. Este evident că $\sigma^{**}(g(X)) = g(X)$, σ^{**} schimbînd doar ordinea factorilor polinomului $g(X) = (X - X_1)(X - X_2)\ldots(X - X_n)$. Pe de altă parte, folosind cealaltă expresie a lui $g(X)$ și cum σ^{**} este omomorfism, rezultă

$$\sigma^{**}(g(X)) = X^n - \sigma^{**}(s_1)X^{n-1} + \ldots + (-1)^n \sigma^{**}(s_n) =$$

$$= X^n - \sigma^*(s_1)X^{n-1} + \ldots + (-1)^n \sigma^*(s_n).$$

Din cele două expresii ale lui $\sigma^{**}(g(X))$ se deduce $\sigma^*(s_i) = s_i$, $1 \leqslant i \leqslant n$, adică s_i $(1 \leqslant i \leqslant n)$ sînt polinoame simetrice.

Polinoamele $s_1, s_2, \ldots, s_n$ se numesc *polinoame simetri elementare (fundamentale)* în nedeterminatele $X_1, X_2, \ldots, X$

Observație. Dacă $X_1^{r_1}X_2^{r_2}\ldots X_n^{r_n}$ este un monom pentru care $r_1 \geqslant r_2 \geqslant \ldots \geqslant r_n$, atunci există doar un număr finit de monoame $X_1^{s_1}X_2^{s_2}\ldots X_n^{s_n}$, pentr care $s_1 \geqslant s_2 \geqslant \ldots \geqslant s_n$ și $X_1^{r_1}X_2^{r_2}\ldots X_n^{r_n} > X_1^{s_1}X_2^{s_2}\ldots X_n^{s_n}$. Într-adevăr, aven $r_1 \geqslant s_1$, deci există doar un număr finit de astfel de numere s_1, iar pentru fiecar s_1 dat există doar cel mult s_1^{n-1} sisteme $(s_2, s_3, \ldots, s_n)$ pentru care $s_1 \geqslant s_2 \geqslant \ldots \geqslant s_n$.

Lema 6.3. *Dacă $f \in A[X_1, X_2, \ldots, X_n]$ este un polinom simetric, iar $aX_1^{k_1}X_2^{k_2}\ldots X_n^{k_n}$ termenul său principal, atunci $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n$.*

Demonstrație. Să presupunem că există i astfel încît $k_i < k_{i+1}$. Cum f este simetric, atunci monomul

$$aX_1^{k_1}\ldots X_i^{k_{i+1}}X_{i+1}^{k_i}\ldots X_n^{k_n}$$

este un termen al lui f, dar evident este mai mare ca $a\,X_1^{k_1}X_2^{k_2}\ldots X_n^{k_n}$, ceea ce este absurd, acesta fiind termenul principal.

Teorema 6.4 (*fundamentală a polinoamelor simetrice*). *Fiecare polinom simetric f din $A[X_1, X_2, \ldots, X_n]$ se poate exprima ca un polinom de polinoame simetrice elementare. Cu alte cuvinte, există un polinom $g \in A[X_1, X_2, \ldots, X_n]$ astfel ca*

$$f = g(s_1, s_2, \ldots, s_n).$$

Mai mult, g este unic determinat prin această proprietate.

Demonstrație. Fie $f \in A[X_1, X_2, \ldots, X_n]$ de grad n astfel încît oricare ar fi $\sigma \in \boldsymbol{\sigma}_n$ avem $\sigma^*(f) = f$. Știm că f se poate scrie în mod unic ca

$$f = f_0 + f_1 + \ldots + f_n,$$

unde f_i sînt polinoame omogene, astfel încît grad $(f_i) = i$. Cum σ^* este un omomorfism, rezultă că

$$\sigma^*(f) = \sigma^*(f_0) + \sigma^*(f_1) + \ldots + \sigma^*(f_n).$$

Dar cum $\sigma^*(f) = f$, din unicitatea scrierii lui f ca sumă de polinoame omogene, rezultă că $\sigma^*(f_i) = f_i$, pentru orice i, adică f_i sînt polinoame simetrice omogene cu gradul egal cu i.

Aşadar, putem presupune, fără a restrînge generalitatea, că f este polinom simetric omogen. Să presupunem de asemenea că $\text{grad}(f) = m$ iar $aX_1^{k_1}X_2^{k_2}\ldots X_n^{k_n}$ $(a \neq 0)$ este termenul său principal. Din lema precedentă rezultă $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n$. Să considerăm produsul $s_1^{d_1}s_2^{d_2}\ldots s_n^{d_n}(d_i \geqslant 0)$. Cum termenul principal al lui s_i este $X_1X_2\ldots X_i$, urmează după lema 4.2 că termenul principal din $s_1^{d_1}s_2^{d_2}\ldots s_n^{d_n}$ este

$$X_1^{d_1+d_2+\ldots+d_n}X_2^{d_2+\ldots+d_n}\ldots X_n^{d_n}.$$

Aşadar, termenul principal al lui $s_1^{k_1-k_2}s_2^{k_2-k_3}\ldots s_n^{k_n}$ este $X_1^{k_1}X_2^{k_2}\ldots X_n^{k_n}$, adică este acelaşi cu al lui f şi deci termenul principal al polinomului simetric

$$f_1 = f - as_1^{k_1-k_2}s_2^{k_2-k_3}\ldots s_n^{k_n}$$

este mai mic decît al lui f.

Să continuăm procedeul pentru f_1. Deoarece există doar un număr finit de monoame de grad m, după un număr finit de paşi procedeul se opreşte. Astfel, se ajunge la o expresie a lui f ca polinom în $s_1, s_2, \ldots, s_n$.

Să demonstrăm unicitatea. Pentru aceasta, observăm mai întîi că este suficient să demonstrăm că dacă $h \in A[X_1, X_2, \ldots, X_n]$ şi $h(s_1, s_2, \ldots, s_n) = 0$, rezultă $h = 0$, deoarece atunci, dacă

$$g(s_1, s_2, \ldots, s_n) = g_1(s_1, s_2, \ldots, s_n),$$

rezultă, punînd $h = g - g_1$, că $h(s_1, s_2, \ldots, s_n) = 0$, deci $h = 0$, adică $g = g_1$. Presupunem deci că $h = \sum a_{i_1i_2\ldots i_n}X_1^{i_1}X_2^{i_2}\ldots X_n^{i_n}$ şi $\sum a_{i_1i_2\ldots i_n}s_1^{i_1}s_2^{i_2}\ldots s_n^{i_n} = 0$ şi să arătăm că toţi coeficienţii sînt nuli. Presupunem prin absurd că există coeficienţi nenuli şi fie $a_{d_1d_2\ldots d_n} \neq 0$ unul dintre aceştia. Atunci, luăm polinomul $s_1^{d_1}s_2^{d_2}\ldots s_n^{d_n}$ care are termenul principal $X_1^{k_1}X_2^{k_2}\ldots X_n^{k_n}$, unde $k_i = d_i + d_{i+1} + \ldots + d_n$, al cărui grad este $m = \sum_{i=1}^{n} k_i = \sum_{i=1}^{n} id_i$. Mai mult, dacă $s_1^{d'_1}s_2^{d'_2}\ldots s_n^{d'_n} \neq s_1^{d_1}s_2^{d_2}\ldots s_n^{d_n}$,

atunci termenii principali respectivi, $X_1^{k'_1} X_2^{k'_2} \dots X_n^{k'_n}$ ş $X_1^{k_1} X_{k_2}^2 \dots X_n^{k_n}$, sînt diferiţi. Într-adevăr, dacă $k'_i = k_i$, pentru $i = 1, 2, \dots, n$, atunci

$$d'_i + d'_{i+1} + \dots + d'_n = d_i + d_{i+1} + \dots + d_n$$

pentru $i = 1, 2, \dots, n$.

De aici rezultă $d'_1 = d_1$, $d'_2 = d_2, \dots, d'_n = d_n$. Deci, termenii principali în $X_1, X_2, \dots, X_n$ ai diferitelor monoame distincte în $s_1, s_2, \dots, s_n$ care apar în expresia lui h nu se reduc. Fie $X_1^{m_1} X_2^{m_2} \dots X_n^{m_n}$ cel mai mare termen principal. Atunci, în expresia polinomului h în funcţie de $X_1, X_2, \dots, X_n$ apare termenul nenul $a_{m_1 m_2 \dots m_n} X_1^{m_1} X_2^{m_2} \dots X_n^{m_n}$, ceea ce contrazice faptul că h este polinomul nul.

Corolarul 6.5. *Fie A un subinel al inelului B şi $f \in A[X]$ un polinom de grad $(f) = n \geqslant 1$. Presupunem că f are rădăcinile $a_1, a_2, \dots a_n$ în B. Dacă $g(X_1, \dots, X_n)$ este un polinom simetric cu coeficienţi în A, atunci $g(a_1, a_2, \dots, a_n) \in A$.*

Demonstraţie. Deoarece $g(X_1, \dots, X_n)$ este simetric, există un polinom $h(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$ astfel încît $g = h(s_1, \dots, s_n)$. Ţinînd seama de relaţiile lui Viète, avem $s_i(a_1, a_2, \dots, a_n) \in A$ $(1 \leqslant i \leqslant n)$ şi deci $g(a_1, a_2, \dots, a_n) = h(s_1(a_1, \dots, a_n), s_2(a_1, \dots, a_n), \dots, s_n(a_1, \dots, a_n))$ este un element din A.

Aplicaţie. *Sume de puteri.* Printre polinoamele simetrice vom considera pe cele de forma

$$t_k = X_1^k + X_2^k + \dots + X_n^k, \quad k = 1, 2, \dots$$

Aceste polinoame, numite *sume de puteri*, trebuie să se exprime, după teorema fundamentală, prin polinoamele simetrice elementare, $s_1, s_2, \dots, s_n$. Vom stabili relaţiile dintre polinoamele $t_1, t_2, \dots$ şi polinoamele $s_1, s_2, \dots, s_n$.

Mai întîi, facem următoarea notaţie. Dacă $X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$ este un monom, atunci prin $s(X_1^{k_1} X_2^{k_2} \dots X_n^{k_n})$ notăm polinomul

$$s(X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}) = \sum_{\sigma \in \mathfrak{S}_n} X_{\sigma(1)}^{k_1} X_{\sigma(2)}^{k_2} \dots X_{\sigma(n)}^{k_n},$$

adică suma termenilor care se obțin făcînd toate permutările nedeterminatelor. Pentru $k = 1, 2, \ldots, n$ următoarele relații sînt imediate:

$$t_{k-1}s_1 = t_k + s(X_1^{k-1}X_2),$$

$$t_{k-j}s_j = s(X_1^{k-j+1}X_2 \ldots X_j) + s(X_1^{k-j}X_2 \ldots X_jX_{j+1}),\ 2 \leqslant j \leqslant k-2,$$

$$t_1s_{k-1} = s(X_1^2X_2 \ldots X_{k-1}) + ks_k,$$

de unde

$$t_k - t_{k-1}s_1 + t_{k-2}s_2 + \ldots + (-1)^k ks_k = 0. \qquad (1)$$

Pentru $k > n$ avem imediat

$$t_{k-1}s_1 = t_k + s(X_1^{k-1}X_2),$$

$$t_{k-j}s_j = s(X_1^{k-j+1}X_2 \ldots X_j) + s(X_1^{k-j}X_2 \ldots X_jX_{j+1}),\ 2 \leqslant j \leqslant n-1,$$

$$t_{k-n}s_n = s(X_1^{k-n+1}X_2 \ldots X_n),$$

de unde

$$t_k - t_{k-1}s_1 + t_{k-2}s_2 + \ldots + (-1)^n t_{k-n}s_n = 0. \qquad (2)$$

Formulele (1) și (2) sînt cunoscute ca *formulele lui Newton*. Ele permit să găsim succesiv expresiile polinoamelor $t_1, t_2, \ldots$ în funcție de $s_1, s_2, \ldots, s_n$. Astfel, $t_1 = s_1$. Pentru $k = 2 \leqslant n$ avem $t_2 - s_1t_1 + 2s_2 = 0$, de unde

$$t_2 = s_1^2 - 2s_2.$$

Pentru $k = 3 \leqslant n$, avem $t_3 - s_1t_2 + s_2t_1 - 3s_3 = 0$, de unde, utilizînd expresiile lui t_1 și t_2, se găsește

$$t_3 = s_1^3 - 3s_1s_2 + 3s_3 \text{ ș.a.m.d.}$$

Dacă în inelul A se poate efectua împărțirea la orice număr natural n, atunci cu formula (1) se pot exprima succesiv polinoamele simetrice elementare $s_1, s_2, \ldots, s_n$ prin primele n sume de puteri $t_1, t_2, \ldots, t_n$. Astfel,

$$s_1 = t_1,$$

$$s_2 = \frac{1}{2}(t_1s_1 - t_2) = \frac{1}{2}(t_1^2 - t_2),$$

$$s_3 = \frac{1}{3}(t_3 - s_1t_2 + s_2t_1) = \frac{1}{6}(t_1^3 - 3t_1t_2 + 3t_3) \text{ ș.a.m.d.}$$

Fracții raționale simetrice. Fie K un corp comutativ ; $K[X_1, X_2, \ldots, X_n]$ inelul polinoamelor de n nedeterminat cu coeficienți în K. Conform propoziției 1.2 din cap. III acesta este un domeniu de integritate. Corpul fracțiilor lu $K[X_1, X_2, \ldots, X_n]$,pe care îl notăm prin $K(X_1, X_2, \ldots, X_n)$, se numește *corpul fracțiilor raționale de n nedeterminate* cu coeficienți în K.O fracție rațională se notează prin $\frac{f}{g}$, unde f, $g \in K[X_1, X_2, \ldots, X_n]$ și $g \neq 0$.

Dacă $\sigma \in \sigma_n$ este o permutare de n elemente, atunci punem $\bar{\sigma}\left(\frac{f}{g}\right) = \frac{\sigma^*(f)}{\sigma^*(g)}$, unde σ^* este definit mai înainte. Observăm că $\bar{\sigma}\left(\frac{f}{g}\right)$ este o fracție rațională care nu depinde de alegerea lui f și g, adică dacă $\frac{f}{g} = \frac{f'}{g'}$, atunci $\bar{\sigma}\left(\frac{f}{g}\right) = \bar{\sigma}\left(\frac{f'}{g'}\right)$. Într-adevăr, din $\frac{f}{g} = \frac{f'}{g'}$ rezultă $fg' = f'g$ și deci $\sigma^*(fg') = \sigma^*(f'g)$, adică $\sigma^*(f)\,\sigma^*(g') = \sigma^*(f')\,\sigma^*(g)$, de unde $\frac{\sigma^*(f)}{\sigma^*(g)} = \frac{\sigma^*(f')}{\sigma^*(g')}$. Astfel, se obține o aplicație : $\bar{\sigma} : K(X_1, X_2, \ldots, X_n) \to K(X_1, X_2, \ldots, X_n)$.

Propoziția 6.6. *Aplicația*

$$\bar{\sigma} : K(X_1, X_2, \ldots, X_n) \to K(X_1, X_2, \ldots, X_n),$$

definită prin

$$\bar{\sigma}\left(\frac{f}{g}\right) = \frac{f(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)})}{g(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)})},$$

este un izomorfism al corpului $K(X_1, X_2, \ldots, X_n)$ pe el însuși.

Demonstrație. Dacă $\frac{f}{g}, \frac{f'}{g'} \in K(X_1, X_2, \ldots, X_n)$, atunci

$$\bar{\sigma}\left(\frac{f}{g}+\frac{f'}{g'}\right)=\bar{\sigma}\left(\frac{fg'+f'g}{gg'}\right)=\frac{\sigma^*(fg'+f'g)}{\sigma^*(gg')}=$$

$$=\frac{\sigma^*(f)\sigma^*(g')+\sigma^*(f')\sigma^*(g)}{\sigma^*(g)\sigma^*(g')}=\frac{\sigma^*(f)}{\sigma^*(g)}+\frac{\sigma^*(f')}{\sigma^*(g')}=$$

$$=\bar{\sigma}\left(\frac{f}{g}\right)+\bar{\sigma}\left(\frac{f'}{g'}\right)$$

şi

$$\bar{\sigma}\left(\frac{f}{g}\cdot\frac{f'}{g'}\right)=\bar{\sigma}\left(\frac{ff'}{gg'}\right)=\frac{\sigma^*(ff')}{\sigma^*(gg')}=\frac{\sigma^*(f)\sigma^*(f')}{\sigma^*(g)\sigma^*(g')}=$$

$$=\frac{\sigma^*(f)}{\sigma^*(g)}\cdot\frac{\sigma^*(f')}{\sigma^*(g')}=\bar{\sigma}\left(\frac{f}{g}\right)\bar{\sigma}\left(\frac{f'}{g'}\right).$$

Deci $\bar{\sigma}$ este un omomorfism de inele. Deoarece

$$\sigma^*: K[X_1, X_2, \ldots, X_n] \to K[X_1, X_2, \ldots, X_n]$$

este un izomorfism, deci σ^* este bijectivă, rezultă uşor că şi $\bar{\sigma}$ este bijectivă. Aşadar $\bar{\sigma}$ este un izomorfism.

Definiţia 6.2. O fracţie raţională $\frac{f}{g}$ din $K(X_1, X_2, \ldots, X_n)$ se numeşte *simetrică* dacă, pentru orice σ din σ_n, avem $\bar{\sigma}\left(\frac{f}{g}\right)=\frac{f}{g}$.

Mulţimea fracţiilor raţionale simetrice formează un subcorp al corpului $K(X_1, X_2, \ldots, X_n)$.

Propoziţia 6.7. *Dacă K este un corp comutativ, atunci pentru orice fracţie raţională simetrică F din $K(X_1, X_2, \ldots, X_n)$ există o fracţie raţională F' din $K(X_1, X_2, \ldots, X_n)$, unic determinată, astfel încît*

$$F = F'(s_1, s_2, \ldots, s_n).$$

Demonstrație. Fie $F = \frac{f}{g}$, $g \neq 0$, o fracție rațională simetrică. Evident, polinomul $\prod_{\sigma \in \sigma_n} \sigma^*(g) = g \prod_{\sigma \neq e} \sigma^*(g)$ (e fiind permutarea identică) este nenul (σ^* este injectiv) și este simetric. Atunci, din $F = \frac{f}{g} = \frac{f \prod_{\sigma \neq e} \sigma^*(g)}{\prod_{\sigma \in \sigma_n} \sigma^*(g)}$ rezultă $f \prod_{\sigma \neq e} \sigma^*(g) = F \prod_{\sigma \in \sigma_n} \sigma^*(g)$ și deoarece F și $\prod_{\sigma \in \sigma_n} \sigma^*(g)$ sînt simetrice, avem că și $f \prod_{\sigma \neq e} \sigma^*(g)$ este simetric. Așadar, dacă F este o funcție rațională simetrică, există f, $g \neq 0$ polinoame simetrice astfel încît $F = \frac{f}{g}$. Deci, după teorema fundamentală a polinoamelor simetrice, există $f', g' \in K[X_1, X_2, \ldots, X_n]$ astfel încît $f = f'(s_1, s_2, \ldots, s_n)$ și $g = g'(s_1, s_2, \ldots, s_n)$. Dacă $F' = \frac{f'}{g'}$, atunci

$$F = F'(s_1, s_2, \ldots, s_n).$$

Pentru a demonstra unicitatea, fie $F'' \in K(X_1, X_2, \ldots, X_n)$ cu $F''(s_1, s_2, \ldots, s_n) = F$. Atunci, dacă $F'' = \frac{f''}{g''}$, $g'' \neq 0$, din relația

$$\frac{f''(s_1, s_2, \ldots, s_n)}{g''(s_1, s_2, \ldots, s_n)} = \frac{f'(s_1, s_2, \ldots, s_n)}{g'(s_1, s_2, \ldots, s_n)}$$

rezultă

$$f''(s_1, s_2, \ldots, s_n)\, g'(s_1, s_2, \ldots, s_n) -$$

$$- f'(s_1, s_2, \ldots, s_n)\, g''(s_1, s_2, \ldots, s_n) = 0$$

și conform unicității de la teorema fundamentală a polinoamelor simetrice, rezultă $f''g' - f'g'' = 0$, adică

$$F'' = \frac{f''}{g''} = \frac{f'}{g'} = F'.$$

§ 7. Teorema fundamentală a algebrei

În acest paragraf demonstrăm un rezultat cunoscut ca teorema fundamentală a algebrei sau teorema lui D'Alembert. Mai întîi, vom demonstra :

Lema 7.1. *Fie f un polinom de grad $n \geqslant 1$, cu coeficienți complecși*

$$f = a_0 + a_1X + \ldots + a_nX^n$$

și

$$m = \max(|a_0|, |a_1|, \ldots, |a_{n-1}|).$$

Atunci, oricare ar fi $\alpha \in \mathbb{C}$, astfel încît $|\alpha| \geqslant \frac{m}{|a_n|} + 1$, avem

$$|a_n\alpha^n| > |a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}|.$$

Demonstrație. Din proprietățile modulului sumei și produsului numerelor complexe (vezi cap. I, § 2) rezultă

$$|a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1}| \leqslant |a_0|+|a_1||\alpha| + \ldots +|a_{n-1}||\alpha|^{n-1} \leqslant$$

$$\leqslant m(1 + |\alpha| + \ldots + |\alpha|^{n-1}) = m\frac{|\alpha|^n - 1}{|\alpha| - 1}.$$

Cum $|\alpha| \geqslant \frac{m}{|a_n|} + 1$, avem $|\alpha| > 1$ și cum

$$\frac{|\alpha|^n - 1}{|\alpha| - 1} < \frac{|\alpha|^n}{|\alpha| - 1},$$

rezultă $|a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}| < m\frac{|\alpha|^n}{|\alpha| - 1}$. Întrucît $|\alpha| \geqslant \frac{m}{|a_n|} + 1$, rezultă $|\alpha||a_n| \geqslant m + |a_n|$ sau $m \leqslant |\alpha||a_n| - |a_n|$ sau încă

$$\frac{m}{|\alpha| - 1} \leqslant |a_n|.$$

De aici avem

$$\frac{m|\alpha|^n}{|\alpha|-1} \leqslant |a_n||\alpha|^n = |a_n\alpha^n|.$$

Deci

$$|a_n\alpha^n| \geqslant \frac{m|\alpha|^n}{|\alpha|-1} > |a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}|,$$

ceea ce trebuia demonstrat.

Din lema precedentă, pentru polinoamele cu coeficienţi reali rezultă

Corolarul 7.2. *Fie* $\in \mathbb{R}[X]$ *un polinom cu coeficienţi reali*

$$f = a_0 + a_1X + \ldots + a_nX^n.$$

Atunci există $r \in \mathbb{R}$, $r > 0$, *suficient de mare astfel încît, oricare ar fi* $y \in \mathbb{R}$ *cu* $|y| > r$, *să avem*

$$f(y)a_n > 0$$

[*adică* $f(y)$ *şi* a_n *au acelaşi semn*].

Teorema 7.3 (*fundamentală a algebrei*). *Orice polinom de grad* $n \geqslant 1$ *cu coeficienţi complecşi are o rădăcină complexă.*

Demonstraţie. Mai întîi, observăm că orice polinom f de grad impar cu coeficienţi reali are cel puţin o rădăcină reală. Într-adevăr, după corolarul precedent, $f(y)$ are semne contrare pentru y pozitiv şi negativ suficient de mare în valoare absolută. Există deci a, $b \in \mathbb{R}$ astfel încît $f(a) < 0$, $f(b) > 0$. Dar cum funcţia $f : \mathbb{R} \to \mathbb{R}$, definită prin $x \to f(x)$, este continuă, după o proprietate fundamentală a funcţiilor continue, rezultă că există $c \in \mathbb{R}$ astfel încît $f(c) = 0$. Deci f are o rădăcină reală.

Acum vom arăta că orice polinom de grad oarecare cu coeficienţi reali are cel puţin o rădăcină complexă. Fie $f \in \mathbb{R}[X]$, grad $(f) = n > 1$ şi fie $k \in \mathbb{N}$ astfel încît 2^k divide n şi 2^{k+1} nu divide n. Demonstraţia se face prin inducţie după k. Cazul $k = 0$ a fost deja considerat, aşa că presupunem $k \geqslant 1$. Presupunem adevărată afirmaţia pentru toate polinoamele cu coeficienţi reali al căror grad se divide la 2^{k-1} şi nu se divide la

2^k. Fie K o extindere a lui $\mathbb{C}$ în care f să aibă toate rădăcinile (vezi propoziția 4.5) și fie $\alpha_1, \alpha_2, \ldots, \alpha_n$ rădăcinile sale în K. Fie a un număr real și elementele

$$\gamma_{ij}^a = \alpha_i\alpha_j + a(\alpha_i + \alpha_j),\ 1 \leqslant i < j \leqslant n.$$

Fie, de asemenea, polinomul

$$h_a = \prod_{1 \leqslant i < j \leqslant n} (X - \gamma_{ij}^a)$$

care are gradul egal cu numărul elementelor γ_{ij}, adică $\dfrac{n(n-1)}{2}$, unde $n = 2^k q$ și 2 nu divide q. Avem $\dfrac{n(n-1)}{2} = 2^{k-1}q(2^k q - 1)$, de unde se vede că 2^{k-1} divide grad (h_a), dar 2^k nu divide grad (h_a). Coeficienții polinomului h_a sînt polinoame simetrice elementare de γ_{ij}^a. Dacă se ține seama de expresiile lui γ_{ij}^a, rezultă că acești coeficienți sînt polinoame de $\alpha_1, \alpha_2, \ldots, \alpha_n$ care sînt chiar simetrice, deoarece efectuarea unei permutări a elementelor $\alpha_1, \alpha_2, \ldots, \alpha_n$ are ca efect schimbarea elementelor γ_{ij}^a între ele. După teorema fundamentală a polinoamelor simetrice rezultă că coeficienții polinomului h_a sînt numere reale. Cum 2^{k-1} divide grad (h_a), iar 2^k nu-l divide, rezultă, conform ipotezei inducției, că h_a are cel puțin o rădăcină complexă, adică există un cuplu (i, j), $i < j$, astfel încît $\gamma_{ij}^a \in \mathbb{C}$. Făcînd pe a să parcurgă mulțimea numerelor reale (care este infinită) și deoarece mulțimea cuplurilor (i, j) cu $1 \leqslant i < j \leqslant n$ este finită, rezultă că există $a, b \in \mathbb{R}$, $a \neq b$, astfel încît $\gamma_{ij}^a, \gamma_{ij}^b \in \mathbb{C}$. Din $\gamma_{ij}^a = \alpha_i\alpha_j + a(\alpha_i + \alpha_j)$ și $\gamma_{ij}^b = \alpha_i\alpha_j + b(\alpha_i + \alpha_j)$ rezultă

$$\gamma_{ij}^a - \gamma_{ij}^b = (a - b)(\alpha_i + \alpha_j) \in \mathbb{C}$$

și deci $\alpha_i + \alpha_j = \dfrac{\gamma_{ij}^a - \gamma_{ij}^b}{a - b} \in \mathbb{C}$. Dar atunci, evident, avem $\alpha_i\alpha_j \in \mathbb{C}$, și deci α_i, α_j sînt rădăcinile unui polinom de gradul doi cu coeficienți complecși. Rădăcinile unui astfel de polinom fiind complexe, rezultă că α_i și α_j sînt numere complexe. Așadar, am arătat că f are rădăcini complexe.

Să considerăm, în final, cazul unui polinom oarecare

$$f = a_0 + a_1X + \ldots + a_nX^n$$

cu coeficienți complecși. Fie, de asemenea, polinomul

$$\bar{f} = \bar{a}_0 + \bar{a}_1 X + \ldots + \bar{a}_n X^n,$$

$\bar{a}_i$ $(0 \leqslant i \leqslant n)$ fiind conjugatul lui a_i. Atunci $f\bar{f}$ este un polinom cu coeficienți reali, deoarece dacă $b_k = \sum_{i+j=k} a_i \bar{a}_j$ $(k = 0, 1, 2, \ldots, 2n)$ este un coeficient oarecare al lui $f\bar{f}$, atunci evident $\bar{b}_k = b_k$. De mai sus, rezultă că există $\alpha \in \mathbb{C}$ cu $(f\bar{f})(\alpha) = f(\alpha)\bar{f}(\alpha) = 0$, de unde $f(\alpha) = 0$ sau $\bar{f}(\alpha) = 0$. Dacă $f(\alpha) = 0$, α este o rădăcină complexă a lui f. Dacă $\bar{f}(\alpha) = 0$, evident $f(\bar{\alpha}) = 0$ și deci $\bar{\alpha}$ este o rădăcină complexă a lui f.

Corolarul 7.4. *Un polinom cu coeficienți complecși este ireductibil dacă și numai dacă este de gradul întîi.*

Demonstrația rezultă din teorema fundamentală a algebrei și propoziția 3.1.

Corolarul 7.5. *Orice polinom f de grad $n \geqslant 1$ cu coeficienți complecși se poate scrie în mod unic, abstracție făcînd de ordinea factorilor, sub forma*

$$f = \alpha(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n),$$

unde $\alpha \neq 0$ și $\alpha_1, \alpha_2, \ldots, \alpha_n$ sînt numere complexe.

Demonstrația rezultă din corolarul precedent și teorema 4.2.

Fie $f \in \mathbb{R}[X]$, $f = a_0 + a_1 X + \ldots + a_n X^n$, un polinom cu coeficienți complecși. După corolarul precedent f se scrie în $\mathbb{C}[X]$ astfel:

$$f = \alpha(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n).$$

Cum aplicația $\mathbb{C}[X] \to \mathbb{C}[X]$ definită prin

$$f = a_0 + a_1 X + \ldots + a_n X^n \to \bar{f} = \bar{a}_0 + \bar{a}_1 X + \ldots + \bar{a}_n X^n$$

este, evident, un automorfism al lui $\mathbb{C}[X]$, rezultă

$$\bar{f} = \bar{\alpha}(X - \bar{\alpha}_1)(X - \bar{\alpha}_2) \ldots (X - \bar{\alpha}_n).$$

În cazul în care $f \in \mathbb{R}[X]$, adică coeficienţii polinomului f sînt reali, avem

$$\bar{f} = \bar{a}_0 + \bar{a}_1 X + \ldots + \bar{a}_n X^n = a_0 + a_1 X + \ldots + a_n X^n = f$$

şi deci în cele două descompuneri diferă doar ordinea factorilor. Deci $\alpha = \bar{\alpha}$ este real şi rădăcinile complexe ale lui f, care nu sînt reale, sînt conjugate două cîte două. Mai mult, două rădăcini conjugate au acelaşi ordin de multiplicitate.

Dacă $\alpha = a + bi$, $b \neq 0$, este un număr complex şi $\bar{\alpha} = a - bi$ este conjugatul său, atunci

$$(X - (a + bi))(X - (a - bi)) = X^2 - 2aX + (a^2 + b^2),$$

care este un polinom cu coeficienţi reali, de gradul doi, avînd discriminantul $4a^2 - 4(a^2 + b^2) = -4b^2 < 0$. Astfel, rezultă :

Propoziţia 7.6. *Orice polinom cu coeficienţi reali de grad* $\geqslant 1$ *se poate descompune în mod unic în* $\mathbb{R}[X]$ *în produs de factori cu coeficienţi reali de gradul întîi şi factori cu coeficienţi reali de gradul doi cu discriminant negativ.*

Corolarul 7.7. *Un polinom cu coeficienţi reali este ireductibil dacă şi numai dacă este de gradul întîi sau de gradul doi cu discriminant negativ.*

Demonstraţie. Avînd în vedere propoziţia precedentă, rămîne de arătat că dacă $aX^2 + bX + c$ este un polinom cu coeficienţi reali şi $b^2 - 4ac < 0$, atunci el este ireductibil. Într-adevăr, dacă presupunem că

$$aX^2 + bX + c = (a_1 X + b_1)(c_1 X + d_1) =$$

$$= a_1 c_1 X^2 + (a_1 d_1 + b_1 c_1) X + b_1 d_1,$$

atunci

$$b^2 - 4ac = (b_1 c_1 - a_1 d_1)^2 \geqslant 0.$$

Astfel, corolarul este probat.

IV

REZOLVAREA ECUAȚIILOR ALGEBRICE DE GRADUL DOI, TREI ȘI PATRU

Considerăm ecuația algebrică de gradul $n \geqslant 1$ cu coeficienți complecși

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \qquad (1)$$

($a_1, a_2, \ldots, a_n$ sînt numere complexe).

Să presupunem, fără a restrînge generalitatea, că coeficientul lui x^n este egal cu 1.

Din teorema fundamentală a algebrei rezultă că ecuația (1) are n rădăcini complexe. Această teoremă are însă neajunsul că nu indică un procedeu de obținere a celor n rădăcini. Toate demonstrațiile care s-au dat acestei teoreme indică numai faptul că pentru ecuația (1) există o rădăcină complexă.

În cele ce urmează ne propunem să arătăm că pentru $n = 2, 3, 4$ se poate da un procedeu de determinare a rădăcinilor ecuației (1) (cazul $n = 1$ este banal : avem ecuația $x + a_1 = 0$ care are rădăcina $x = -a_1$).

§ 1. Numere complexe exprimabile prin radicali

Noțiunile pe care le vom prezenta aici vor fi date cît mai intuitiv posibil, iar definițiile lor în mod riguros vor fi date în cap. VII.

Considerăm formulele (expresiile algebrice) de forma

$$R(t_1, t_2, \ldots, t_n) \qquad (2)$$

care conțin în afara simbolurilor de operații aritmetice (adunarea, înmulțirea, împărțirea) numai semnele $\sqrt[k]{\ }$ (extragerea rădăcinii de ordinul k dintr-nn număr complex).

Exemplu. Expresiile algebrice

$$t_1 + t_2 t_3,\quad t_1 + \sqrt{t_2},\quad t_1 + \sqrt[3]{t_1 - \sqrt{t_2}},\quad t_1^2 t_3' + \sqrt{t_2} - \sqrt[6]{t_3 - t_1}$$

conțin numai simbolurile operațiilor aritmetice (adunarea, înmulțirea, împărțirea) și simbolul extragerii rădăcinii de ordinul k.

Fie $R(t_1, t_2, \ldots, t_n)$ o expresie algebrică de tipul (2). Cînd mărimilor $t_1, t_2, \ldots, t_n$ dăm valorile $t_1 = a_1, \ldots, t_n = a_n$, $R(a_1, a_2, \ldots, a_n)$ are mai multe valori (un număr finit), ținînd seama de multiformitatea extragerii rădăcinii de ordinul k.

Se spune că un număr complex z *se exprimă prin radicali* din numerele complexe $a_1, a_2, \ldots, a_n$ dacă există o expresie de tipul (2) astfel încît z să fie una din valorile lui $R(a_1, a_2, \ldots, a_n)$.

Dacă $a_1, a_2, \ldots, a_n$ sînt numere raționale arbitrare, atunci vom spune simplu că z *se exprimă prin radicali.*

Exemple. 1. Numărul complex $1 + i$ se exprimă prin radicali. Într-adevăr, dacă considerăm expresia $R(t_1, t_2) = t_1 + \sqrt{t_2}$, unde $t_1 = 1$ și $t_2 = -1$, obținem că $R(1, -1)$ are două valori $1 + i$ și $1 - i$. Deci $1 + i$ se exprimă prin radicali.

2. Numărul $\sqrt[3]{2} + \sqrt[7]{5} - \sqrt{3}$ se exprimă prin radicali. Într-adevăr, considerînd expresia $R(t_1, t_2, t_3) = \sqrt[3]{t_1} + \sqrt[7]{t_2} - \sqrt{t_3}$, unde $t_1 = 2$, $t_2 = 5$ și $t_3 = 3$, una din valorile $R(2, 5, 3)$ este numărul real $\sqrt[3]{2} + \sqrt[7]{5} - \sqrt{3}$.

§ 2. Ce înseamnă a rezolva o ecuație prin radicali

Spunem că o *rădăcină z_0 a ecuației* (1) *se exprimă prin radicali* dacă există o formulă de tipul (2), $R(t_1, t_2, \ldots, t_n)$, astfel încît z_0 să fie una din valorile expresiei $R(a_1, a_2, \ldots, a_n)$, adică z_0 se exprimă prin radicali din numerele complexe $a_1, a_2, \ldots, a_n$. Dacă orice rădăcină a ecuației (1) se exprimă prin radicali, atunci spunem că *ecuația* (1) *se rezolvă prin radicali*. Dacă există o formulă de tipul (2), $R(t_1, t_2, \ldots, t_n)$, astfel încît pentru orice numere complexe $a_1, a_2, \ldots, a_n$ ecuația

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

are rădăcinile exprimabile prin radicali prin intermediul expresiei $R(t_1, t_2, \ldots, t_n)$, atunci vom spune că $R(t_1, t_2, \ldots, t_n)$ este *formula de rezolvare a ecuației de gradul n.*

Observație. Presupunem că pentru ecuația $x^n + a_1x^{n-1} + \ldots + a_n=0$ rădăcinile sale se exprimă prin radicali prin intermediul formulei $R(t_1, t_2, \ldots, t_n)$, adică rădăcinile sale sînt o parte din valorile expresiei $R(a_1, a_2, \ldots, a_n)$. O problemă care se pune este de a distinge din mulțimea valorilor expresiei $R(a_1, a_2, \ldots, a_n)$ cele care sînt rădăcinile ecuației date. Acest lucru se face pentru fiecare caz particular în parte.

§ 3. Formulele de rezolvare pentru ecuațiile de gradul doi, trei și patru

— *Ecuația de gradul doi.* Făcînd în (1) $n = 2$, obținem ecuația de gradul doi cu coeficienți complecși

$$x^2 + a_1x + a_2 = 0.$$

Această ecuație se poate scrie sub forma

$$\left(x + \frac{a_1}{2}\right)^2 + \left(a_2 - \frac{a_1}{4}\right)^2 = 0$$

sau

$$\left(x + \frac{a_1}{2}\right)^2 = \frac{a_1^2}{4} - a_2,$$

de unde

$$x + \frac{a_1}{2} = \pm\sqrt{\frac{a_1^2}{4} - a_2}$$

sau

$$x = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_2}$$

sau încă

$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2}}{2}. \tag{3}$$

Egalitatea (3) arată că ecuația de gradul doi este rezolvabilă prin radicali iar membrul al doilea al egalității (2) constituie *formula de rezolvare a ecuației de gradul doi.*

Exemplu. Să se rezolve ecuația

$$x^2 - x + (1 - i) = 0.$$

Aplicînd formula stabilită mai sus, obținem

$$x = \frac{1 \pm \sqrt{1 - 4(1 - i)}}{2} = \frac{1 \pm \sqrt{4i - 3}}{2}.$$

Dar $\sqrt{-3 + 4i} = \pm (1 + 2i)$. Deci rădăcinile ecuației sînt

$$x_1 = 1 + i \text{ și } x_2 = -i.$$

— *Ecuația de gradul trei.* Fie ecuația de gradul trei cu coeficienți complecși

$$x^3 + a_1x^2 + a_2x + a_3 = 0. \tag{4}$$

Înlocuind în (4) necunoscuta x printr-o nouă necunoscută y legată de x prin relația

$$y = x + \frac{a_1}{3},$$

obținem o ecuație în necunoscuta y de gradul trei în care coeficientul termenului în y^2 este egal cu zero, adică o ecuație de forma

$$y^3 + py + q = 0. \tag{4'}$$

Se vede ușor că rezolvarea ecuației (4) revine la rezolvarea ecuației (4'). În concluzie, vom căuta să indicăm o metodă de rezolvare pentru ecuația de gradul trei de forma (4').

După teorema fundamentală a algebrei, ecuația (4') posedă trei rădăcini complexe. Fie y_0 una dintre aceste rădăcini. Considerăm polinomul în nedeterminata u

$$f_0(u) = u^2 - y_0u - \frac{p}{3}.$$

Fie α, β rădăcinile ecuației $f_0(u) = 0$. Relațiile lui Viète ne dau

$$\alpha + \beta = y_0, \quad \alpha\beta = -\frac{p}{3}.$$

Cum $y^3_0 + py_0 + q = 0$, obţinem că

$$(\alpha + \beta)^3 + p(\alpha + \beta) + q = 0$$

sau

$$\alpha^3 + 3\alpha^2\beta + 3\alpha\beta^2 + \beta^3 + p\alpha + p\beta + q = 0,$$

de unde

$$\alpha^3 + \beta^3 + (\alpha + \beta)(3\alpha\beta + p) + q = 0.$$

Dar $3\,\alpha\beta + p = 0$ şi atunci avem $\alpha^3 + \beta^3 = -q$. Deci obţinem sistemul de ecuaţii în α şi β :

$$\left.\begin{aligned} \alpha^3 + \beta^3 &= -q \\ \alpha\beta &= -\frac{p}{3} \end{aligned}\right\}$$

de unde obţinem sistemul de ecuaţii

$$\left.\begin{aligned} \alpha^3 + \beta^3 &= -q \\ \alpha^3\beta^3 &= -\frac{p^3}{27} \end{aligned}\right\}$$

Rezultă că α^3 şi β^3 sînt rădăcinile ecuaţiei de gradul doi în t :

$$t^2 + qt - \frac{p^3}{27} = 0,$$

care rezolvată ne dă

$$t = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

de unde obţinem

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\,;\ \beta = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad (5)$$

iar

$$y_0 = \alpha + \beta = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \quad (6)$$

Expresia $\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$ se numeşte *formula lui Cardano* de rezolvare a ecuaţiei de gradul trei. Rezultă că ecuaţia de gradul trei este rezolvabilă prin radicali. Ţinînd seama de faptul că rădăcina cubică dintr-un număr complex are trei valori complexe, formula lui Cardano ne dă şase valori complexe. Trebuie să distingem dintre aceste valori care sînt rădăcinile ecuaţiei (4').

Considerăm formulele (5). Fie α_1 una dintre cele trei valori ale lui α date de formulele (5). Dacă ε şi ε^2 sînt rădăcinile cubice ale unităţii diferite de 1, atunci celelalte valori ale lui α sînt

$$\alpha_2 = \varepsilon\alpha_1 \text{ şi } \alpha_3 = \varepsilon^2\alpha_1.$$

Fie β_1, β_2, β_3 valorile lui β date de formulele (5). Avem

$$\beta_2 = \varepsilon\beta_1 \text{ şi } \beta_3 = \varepsilon^2 \cdot \beta_1.$$

Dar trebuie ca $\alpha\beta = -\frac{p}{3}$. Să presupunem că β_1 este valoarea corespunzătoare lui α_1 $\left(\text{adică } \alpha_1 \beta_1 = -\frac{p}{3}\right)$. Se vede uşor că

$$\alpha_2\beta_3 = (\varepsilon\alpha_1)(\varepsilon^2\beta_1) = \varepsilon^3(\alpha\beta_1) = -\frac{p}{3}$$

şi

$$\alpha_3\beta_2 = (\varepsilon^2\alpha_1)(\varepsilon\beta_1) = -\frac{p}{3},$$

deoarece $\varepsilon^3 = 1$. Deci β_3 este valoarea corespunzătoare lui α_2 şi β_2 este valoarea corespunzătoare lui α_3. Rezultă că rădăcinile ecuaţiei (4') sînt

$$\left.\begin{aligned} y_1 &= \alpha_1 + \beta_1 \\ y_2 &= \alpha_2 + \beta_3 = \varepsilon\alpha_1 + \varepsilon^2\beta_1 \\ y_3 &= \alpha_3 + \beta_2 = \varepsilon^2\alpha_1 + \varepsilon\beta_1 \end{aligned}\right\} \quad (7)$$

— *Ecuaţia de gradul patru.* Considerăm în ecuaţia (1) $n = 4$:

$$x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0. \quad (8)$$

Înlocuind în (8) necunoscuta x cu necunoscuta y dată de egalitatea

$$y = x + \frac{a_1}{4},$$

obținem ecuația de forma

$$y^4 + py^2 + qy + r = 0. \tag{9}$$

Fie m un parametru. Avem egalitatea evidentă

$$Y^4 + pY^2 + qY + r = \left(Y^2 + \frac{p}{2} + m\right)^2 + qY + r = \frac{p^2}{4} -$$

$$- m^2 - 2mY^2 - pm$$

sau încă

$$Y^4 + pY^2 + qY + r = \left(Y^2 + \frac{p}{2} + m\right)^2 - \left[2mY^2 - qY + \right.$$

$$\left. + \left(m^2 + pm - r + \frac{p^2}{4}\right)\right].$$

Alegem pe m așa încît polinomul în Y

$$f(Y) = 2mY^2 - qY + \left(m^2 + pm - r + \frac{p^2}{4}\right)$$

să fie pătratul unui polinom de gradul întîi. Pentru aceasta trebuie ca discriminantul ecuației $f(y) = 0$ să fie nul, adică

$$q^2 - 8m\left(m^2 + pm - r + \frac{p^2}{4}\right) = 0$$

sau

$$8m^3 + 8pm^2 + 8\left(r - \frac{p^2}{4}\right)m - q^2 = 0, \tag{9'}$$

care este o ecuaţie de gradul trei în m. Ecuaţia (9′) are o rădăcină complexă, fie aceasta m_0. Mai mult, această rădăcină se exprimă prin radicali. Pentru m_0 avem

$$f(Y) = 2m_0\left(Y - \frac{q}{4m_0}\right)^2.$$

În acest caz ecuaţia (9) devine

$$\left(y^2 + \frac{p}{2} + m_0\right)^2 - 2m_0\left(y - \frac{q}{4m_0}\right)^2 = 0$$

care se descompune în două ecuaţii de gradul doi:

$$y^2 - \sqrt{2m_0}\,y + \left(\frac{p}{2} + m_0 + \frac{q}{2\sqrt{2m_0}}\right) = 0, \qquad (10)$$

$$y^2 + \sqrt{2m_0}\,y + \left(\frac{p}{2} + m_0 - \frac{q}{2\sqrt{2m_0}}\right) = 0. \qquad (10')$$

Ecuaţiile (10) şi (10′) ne arată că ecuaţia de gradul patru este rezolvabilă prin radicali. Nu vom da aici formule de rezolvare a ecuaţiei de gradul patru deoarece sînt destul de complicate şi n-au nici o utilitate practică.

§ 4. Natura rădăcinilor ecuaţiei de gradul trei cu coeficienţi reali

Fie din nou ecuaţia de gradul n

$$x^n + a_1x^{n-1} + \ldots + a_n = 0.$$

Notăm cu $x_1, x_2, \ldots, x_n$ rădăcinile acestei ecuaţii. Numărul complex

$$d = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2$$

se numeşte *discriminantul ecuaţiei* (1).

Este uşor de văzut că are loc egalitatea

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ \dots & \dots & \dots & \dots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{vmatrix} = \prod_{i>j} (x_i - x_j). \qquad (11)$$

Primul membru al egalităţii (10) este determinantul Vandermonde. Să notăm cu $\mathfrak{A}$ matricea

$$\mathfrak{A} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ \dots & \dots & \dots & \dots \\ x_1^{n-1} & x_2^{n-2} & \dots & x_n^{n-1} \end{pmatrix}$$

şi cu $\mathfrak{A}^*$ matricea transpusă. Fie $|\mathfrak{A}|$ determinantul matricei $\mathfrak{A}$. Este cunoscut că $|\mathfrak{A}| = |\mathfrak{A}^*|$ şi deci $d = |\mathfrak{A}|\,|\mathfrak{A}^*| = |\mathfrak{A}\,\mathfrak{A}^*|$.Dar

$$d = |\mathfrak{A}\mathfrak{A}^*| = \begin{vmatrix} n & t_1 & t_2 & \dots & t_{n-1} \\ t_1 & t_2 & t_3 & \dots & t_n \\ t_2 & t_3 & t_4 & \dots & t_{n+1} \\ \dots & \dots & \dots & \dots & \dots \\ t_{n-1} & t_n & t_{n+1} & \dots & t_{2n-2} \end{vmatrix} \qquad (12)$$

unde $t_i = x_1^i + x_2^i + \dots + x_n^i$ sînt sumele de puteri ale lui Newton. Relaţiile lui Viète ne dau

$$\sum_{i=1}^{n} x_i = -a_1, \quad \sum_{i<j} x_i x_j = a_2, \dots, x_1 x_2 \dots x_n = (-1)^n a_n.$$

Dacă $a_1, a_2, \dots, a_n$ sînt numere reale, atunci din (12) şi după aplicaţia din cap. III. 16, obţinem că d este un număr real ce se exprimă în funcţie de $a_1, a_2, \dots, a_n$.

Ne propunem să calculăm discriminantul d pentru $n = 2, 3$. Pentru $n = 2$, avem ecuaţia $x^2 + a_1 x + a_2 = 0$,

$$d = (x_1 - x_2)^2 = x_1^2 + x_2^2 - 2x_1x_2 = (x_1 + x_2)^2 - 4x_1x_2.$$

Dar $x_1 + x_2 = -a_1$ și $x_1 x_2 = a_2$. Atunci $d = a_1^2 - 4a_2$.

Pentru $n = 3$, avem ecuația $x^3 + a_1 x^2 + a_2 x + a_3 = 0$,

$$d = (x_1 - x_2)^2 (x_2 - x_3)^2 (x_1 - x_3)^2.$$

Ținînd seama de relațiile lui Viète

$$x_1 + x_2 + x_3 = -a_1,\ x_1 x_2 + x_2 x_3 + x_3 x_1 = a_2,\ x_1 x_2 x_3 = -a_3,$$

obținem

$$d = -4a_1^3 a_3 + a_1^2 a_2^2 + 18 a_1 a_2 a_3 - 4a_3^2 \quad 27a_3^2.$$

— *Discuția rădăcinilor ecuației de gradul trei* $x^3 + px + q = 0$. Este clar că natura rădăcinilor ecuației $x^3 + a_1 x^2 + a_2 x + a_3 = 0$ se reduce la a determina natura rădăcinilor ecuației reduse în care $a_1 = 0$. Așadar, vom face aici discuția rădăcinilor ecuației

$$x^3 + px + q = 0. \tag{13}$$

Discriminantul acestei ecuații este

$$d = -(4p^3 + 27q^2) = -108\left(\frac{q^2}{4} + \frac{p^3}{27}\right).$$

Cazul $d < 0$. Ecuația fiind de gradul trei are cel puțin o rădăcină reală; fie aceasta x_1. Deoarece

$$d = (x_1 - x_2)^2 (x_2 - x_3)^2 (x_1 - x_3)^2 < 0,$$

x_2 și x_3 sînt numere complexe conjugate. Deci pentru $d < 0$ ecuația (13) are o rădăcină reală și două complexe conjugate.

Cazul $d = 0$. Se vede clar că ecuația (13) are cel puțin două rădăcini egale. Cum o rădăcină este reală, rezultă că toate trei sînt reale (din care cel puțin două sînt egale).

Cazul $d > 0$. Avem

$$(x_1 - x_2)^2 (x_2 - x_3)^2 (x_1 - x_3)^2 > 0.$$

Presupunem că x_1 este reală. Dacă x_2 și x_3 ar fi complexe conjugate, am putea scrie

$$x_2 = a + ib \text{ și } x_3 = a - ib \text{ cu } b \neq 0.$$

În acest caz am avea

$$d = (x_1 - a - ib)^2 (-b^2) (x_1 - a + ib)^2 = [(x_1 - a) -$$

$$-ib]^2 [(x_1 - a) + ib]^2 (-b^2) = (-b^2) [(x_1 - a)^2 + b^2]^2 < 0,$$

deci am ajuns la o contradicție. Rezultă că în cazul $d > 0$ ecuația (13) are trei rădăcini reale distincte.

§ 5. Metoda Lagrange de rezolvare a ecuațiilor algebrice de grad $\leqslant 4$

În acest paragraf vom prezenta metoda Lagrange de rezolvare a ecuațiilor de grad $\leqslant 4$. Ideea acestei metode constă în a reduce o ecuație de acest tip la un număr de ecuații algebrice a căror rezolvare este mai simplă. Aceasta mai are importanță prin faptul că aici se găsește ideea dezvoltării teoriei lui Galois.

— *Subgrupul invariant al unei fracții raționale*

Fie $F(X_1, X_2, \ldots, X_n) = \dfrac{f(X_1, \ldots, X_n)}{g(X_1,) \ldots, X_n}$ o fracție rațională cu coeficienți numere complexe. Notăm $\sigma F(X_1, \ldots, X_n) = F(X_{\sigma(1)} \ldots X_{\sigma(n)})$, unde $\sigma \in \boldsymbol{\sigma}_n$. Se spune că permutarea σ *invariază fracția rațională* $F(X_1, X_2, \ldots, X_n)$ dacă $F(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}) = F(X_1, \ldots, X_n)$. Vom nota cu H_F mulțimea permutărilor ce invariază pe F.

Propoziția 5.1. *H_F este un subgrup al lui $\boldsymbol{\sigma}_n$.*

Demonstrație. Fie $\sigma \in H_F$; atunci avem $F(X_{\sigma(1)}, X_{\sigma(2)} \ldots \ldots, X_{\sigma(n)}) = F(X_1, \ldots, X_n)$. Rezultă

$$F(X_{\sigma^{-1}(1)}, \ldots, X_{\sigma^{-1}(n)}) = F(X_{\sigma^{-1}(\sigma(1))}, \ldots, X_{\sigma^{-1}(\sigma(n))}) = F(X_1, X_2, \ldots, X_n)$$

și deci $\sigma^{-1} \in H_F$.

Dacă σ, $\tau \in H_F$, atunci avem

$$F(X_{\tau(1)}, \ldots, X_{\tau(n)}) = F(X_1, \ldots, X_n),$$

de unde rezultă

$$F(X_{\sigma(\tau(1))}, \ldots, X_{\sigma(\tau(n))}) = F(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = F(X_1, \ldots, X_n)$$

și deci $F(X_{(\sigma\tau)(1)}, \ldots, X_{(\sigma\tau)(n)}) = F(X_1, \ldots, X_n)$, adică $\sigma\tau \in H_F$. Deci H_F este subgrup al lui σ_n.

Subgrupul H_F se numește *subgrupul invariant* pentru fracția rațională $F(X_1, \ldots, X_n)$.

Invers, dat fiind un subgrup H a lui σ_n, o fracție rațională $F(X_1, \ldots, X_n)$ se spune că este un *invariant* pentru H dacă $H = H_F$.

Observație $H_F = \sigma_n$ dacă și numai dacă F este o fracție simetrică.

Exemple. 1. Fie polinomul $F(X_1, X_2, X_3) = X_1 + X_2 - X_3$. În acest caz H_F este subgrupul lui σ_3 format din permutările e și $(1, 2)$.

2. Fie polinomul $A(X_1, X_2, X_3, X_4) = X_1X_2 + X_3X_4$. Atunci H_A este următorul subgrup al lui σ_4:

$H_F = \{e, (1, 2), (3, 4), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 3, 2, 4), (1, 4, 2, 3)\}$.

Într-adevăr:

$$\begin{aligned}
&\sigma = e, && \sigma A = A,\\
&\sigma = (1, 2), && \sigma A = X_2X_3 + X_3X_4 = A,\\
&\sigma = (3, 4), && \sigma A = X_1X_2 + X_4X_3 = A,\\
&\sigma = (1, 2)(3, 4), && \sigma A = X_2X_1 + X_4X_3 = A,\\
&\sigma = (1, 3)(2, 4), && \sigma A = X_3X_4 + X_1X_2 = A,\\
&\sigma = (1, 4)(2, 3), && \sigma A = X_4X_3 + X_2X_1 = A,\\
&\sigma = (1, 3, 2, 4), && \sigma A = X_3X_4 + X_2X_1 = A,\\
&\sigma = (1, 4, 2, 3), && \sigma A = X_4X_3 + X_1X_2 = A.
\end{aligned}$$

Subgrupul H_G obținut astfel se notează σ_8 și este de ordinul opt.

3. Fie polinomul $B(X_1, X_2, X_3) = (X_1 + \varepsilon X_2 + \varepsilon^2 X_3)^3$, unde ε este o rădăcină cubică a unității $\neq 1$. Subgrupul invariant H_B al lui $B(X_1, X_2, X_3)$ este format din permutările

$$H_B = \{e, (1, 2, 3), (1, 3, 2)\}.$$

Într-adevăr

$$\sigma = e, \ \sigma B = B,$$

$$\begin{aligned}
\sigma = (1, 2, 3),\ \sigma B &= (X_2 + \varepsilon X_3 + \varepsilon^2 X_1)^3 = [\varepsilon^2(X_1 + \varepsilon^2 X_3 + \varepsilon X_2)]^3 =\\
&= \varepsilon^6(X_1 + \varepsilon X_2 + \varepsilon^2 X_3)^3 = (X_1 + \varepsilon X_2 + \varepsilon^2 X_3)^3 = B,
\end{aligned}$$

$$\begin{aligned}
\sigma = (1, 3, 2),\ \sigma B &= (X_3 + \varepsilon X_1 + \varepsilon^2 X_2)^3 = [\varepsilon(X_1 + \varepsilon X_2 + \varepsilon^2 X_3)]^3 =\\
&= \varepsilon^3(X_1 + \varepsilon X_2 + \varepsilon^2 X_3)^3 = (X_1 + \varepsilon X_2 + \varepsilon^2 X_3)^3 = B.
\end{aligned}$$

Se constată că celelalte permutări $(1, 2)$, $(1, 3)$ și $(2, 3)$ ale lui σ_3 nu invariază pe B, deci nu aparțin lui H_B.

Propoziția 5.2. *Fie $F(X_1, \ldots, X_n)$ o fracție rațională cu H_F subgrupul invariant și fie $\hat{\pi} = \pi H_F$ o clasă de echivalență la stînga modulo subgrupul H_F. Atunci pentru orice $\sigma \in \pi H_F$ avem*

$$\sigma F(X_1, \ldots, X_n) = \pi F(X_1, \ldots, X_n).$$

Demonstrație. Dacă $\sigma \in \pi H_F$, atunci există $\tau \in H_F$ astfel încît $\sigma = \pi\tau$. Atunci

$$\sigma F(X_1, \ldots, X_n) = (\pi\tau) F(X_1, \ldots, X_n) = \pi F(X_{\tau(1)}, \ldots, X_{\tau(n)}) =$$
$$= \pi F(X_1, \ldots, X_n) = F(X_{\pi(1)}, \ldots, X_{\pi(n)}).$$

Teorema 5.3. *Fie $F(X_1, \ldots, X_n)$ o fracție rațională cu H_F subgrupul invariant asociat. Atunci $F(X_1, \ldots, X_n)$ este rădăcină a unui polinom de gradul $p = [\sigma_n : H_F]$ cu coeficienți în inelul polinoamelor simetrice în nedeterminatele $X_1, X_2, \ldots, X_n$.*

Demonstrație. Fie $\hat{\pi}_1, \ldots, \hat{\pi}_p$ clasele de echivalență la stînga modulo subgrupul H_F. Putem presupune că $\pi_1 = e$. Să punem

$$F_i(X_1, \ldots, X_n) = \pi_i F(X_1, \ldots, X_n) = F(X_{\pi_i(1)}, \ldots, X_{\pi_i(n)}).$$

Cum $\pi_1 = e$, atunci $F_1(X_1, \ldots, X_n) = F(X_1, \ldots, X_n)$.

Considerăm polinomul de gradul p:

$$P(Y) = \prod_{i=1}^{p} (Y - F_i(X_1, \ldots, X_n)).$$

Fie σ o permutare arbitrară a lui σ_n. Atunci $\sigma F_i(X_1, \ldots, X_n)$ este una dintre valorile $F_1, F_2, \ldots, F_p$. Într-adevăr

$$\sigma F_i(X_1, \ldots, X_n) = \sigma\pi_i F(X_1, \ldots, X_n).$$

Dar $\sigma\pi_i$ aparține unei clase de echivalență, fie aceasta $\hat{\pi}_j$. Din propoziția 5.2 obținem

$$\sigma\pi_i F(X_1, \ldots, X_n) = \pi_j F(X_1, \ldots, X_n) = F_j(X_1, \ldots, X_n).$$

Pe de altă parte, dacă $i \neq j$, avem $\sigma F_i \neq \sigma F_j$. Într-adevăr, dacă

$$\sigma Fi = \sigma F_j, \text{ atunci } \sigma^{-1}(\sigma F_i) = \sigma^{-1}(\sigma F_j) \text{ și deci } F_i = F_j.$$

Valorile $F_1, F_2, \ldots, F_p$ sînt distincte. Într-adevăr, dacă $F_i = F_j$, atunci $\pi_i F = \pi_j F$, de unde $\pi_j^{-1}\pi_i F = F$ și deci $\pi_j^{-1}\pi_i \in H_F$, ceea ce implică $\hat{\pi}_i = \hat{\pi}_j$, adică se obține o contradicție.

Deci rezultă egalitatea $\{\sigma F_1, \sigma F_2, \ldots, \sigma F_p\} = \{F_1, F_2, \ldots, F_p\}$ oricare ar fi $\sigma \in \boldsymbol{\sigma}_n$.

Scriem polinomul (14) sub forma

$$P(Y) = Y^p - A_1 Y^{p-1} + A_2 Y^{p-2} + \ldots + (-1)^p A_p, \quad (15)$$

unde

$$A_1 = F_1 + F_2 + \ldots + F_p = \sum_{i=1}^{p} F_i,$$

$$A_2 = \sum_{1 \leqslant i < j \leqslant p} F_i F_j,$$

$$\ldots\ldots\ldots\ldots$$

$$A_p = F_1 F_2 \ldots F_p.$$

Fie σ o permutare arbitrară a lui $\boldsymbol{\sigma}_n$. Ținînd seama de (15), obținem

$$\sigma A_1 = \sum_{i=1}^{p} \sigma F_i = \sum_{i=1}^{p} F_i = A_1,$$

$$\sigma A_2 = \sum_{1 \leqslant i < j \leqslant p} \sigma F_i \, \sigma F_j = \sum_{1 \leqslant i < j \leqslant p} F_i F_j = A_2,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sigma A_p = \sigma F_1 \, \sigma F_2 \ldots \sigma F_p = F_1 F_2 \ldots F_p = A_p.$$

Rezultă că polinoamele $A_1, A_2, \ldots, A_p$ sînt simetrice. Dar $F_1 = F$ este o rădăcină a ecuației (14), ceea ce termină demonstrația.

— ***Rezolvarea ecuației de gradul al treilea prin metoda lui Lagrange.*** Considerăm ecuația de gradul trei (forma redusă)

$$x^3 + px + q = 0, \quad (16)$$

unde p, q sînt numere complexe. Considerăm expresia

$$B = (X_1 + \varepsilon X_2 + \varepsilon^2 X_3)^3,$$

unde ε este o rădăcină cubică a unității, diferită de 1. Am văzut că subgrupul invariant pentru B este

$$H_B = \{e, (1, 2, 3), (1, 3, 2)\}$$

(a se vedea exemplul 3). Cum H_B este de indice doi în σ_3, atunci conform teoremei 5.3, B verifică o ecuaţie de gradul doi cu coeficienţi polinoame simetrice în X_1, X_2, X_3. Să determinăm această ecuaţie. Clasele de echivalenţă la stînga modulo subgrupul H_B sînt două:

$$\hat{e} = e \cdot H_B = H_B = \{e, (1, 2, 3), (1, 3, 2)\},$$

$$\widehat{(1, 2)} = (1, 2) H_B = \{(1, 2), (1, 3), (2, 3)\}.$$

Cele două valori ale lui B sînt

$$B_1 = e \cdot B = B = (X_1 + \varepsilon X_2 + \varepsilon^2 X_3)^3,$$

$$B_2 = (1, 2) B = (X_2 + \varepsilon X_1 + \varepsilon^2 X_3)^3.$$

Ecuaţia de gradul doi pe care o verifică B este

$$(z - B_1)(z - B_2) = 0$$

sau

$$z^2 - (B_1 + B_2) z + B_1 B_2 = 0.$$

Dar

$$B_1 + B_2 = (X_1 + \varepsilon X_2 + \varepsilon^2 X_3)^3 + (X_2 + \varepsilon X_1 + \varepsilon^2 X_3)^3 =$$
$$= 2 s_1^3 - 9 s_1 s_2 + 27 s_3$$

şi $B_1 B_2 = (s_1^2 - 3 s_2)^3$, unde

$$s_1 = X_1 + X_2 + X_3, \; s_2 = X_1X_2 + X_1X_3 + X_2X_3, \; s_3 = X_1X_2X_3.$$

Deci B verifică ecuaţia

$$z^2 - (2s_1^3 - 9 s_1 s_2 + 27 s_3) z + (s_1^2 - 3s_2)^3 = 0, \qquad (17)$$

coeficienţii săi fiind polinoame simetrice (deci rezultatul corespunde teoriei). Să notăm $L_{\varepsilon X} = X_1 + \varepsilon X_2 + \varepsilon^2 X_3$. Se vede uşor că $B_1 = L_{\varepsilon X}^3$ şi $B_2 = L_{\varepsilon^2 X}^3$, unde B_1 şi B_2 sînt rădăcinile ecuaţiei (17). Dacă x_1, x_2, x_3 sînt rădăcinile ecuaţiei (16), să

notăm cu $L_{\varepsilon x}$ valoarea lui $L_{\varepsilon X}$ cînd facem $X_1 = x_1$, $X_2 = x_2$, $X_3 = x_3$. Se obține sistemul de ecuații

$$\left.\begin{aligned} x_1 + x_2 + x_3 &= 0 \\ x_1 + \varepsilon x_2 + \varepsilon^2 x_3 &= L_{\varepsilon x} \\ x_1 + \varepsilon^2 x_2 + \varepsilon x_3 &= L_{\varepsilon^2 x} \end{aligned}\right\}. \tag{18}$$

Determinantul acestui sistem este

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & \varepsilon & \varepsilon^2 \\ 1 & \varepsilon^2 & \varepsilon \end{vmatrix} = (\varepsilon^2 - \varepsilon^4) - (\varepsilon - \varepsilon^2) + (\varepsilon^2 - \varepsilon) = \varepsilon^2 - \varepsilon - \varepsilon + \varepsilon^2 + \varepsilon^2 - \varepsilon = 3(\varepsilon^2 - \varepsilon) \neq 0.$$

Deci sistemul (18) are o soluție unică. Rezolvînd acest sistem, obținem soluția

$$x_1 = \frac{1}{3}(L_{\varepsilon x} + L_{\varepsilon^2 x}), \quad x_2 = \frac{1}{3}(\varepsilon^2 L_{\varepsilon x} + \varepsilon L_{\varepsilon^2 x}),$$
$$x_3 = \frac{1}{3}(\varepsilon L_{\varepsilon x} + \varepsilon^2 L_{\varepsilon^2 x}). \tag{19}$$

Așadar rezolvarea ecuației de gradul trei (16) se reduce la determinarea lui $L_{\varepsilon x}$ și $L_{\varepsilon^2 x}$.

Să notăm cu b_1 și b_2 valorile lui B_1, respectiv B_2 pentru $X_1 = x_1$, $X_2 = x_2$, $X_3 = x_3$. Atunci b_1 și b_2 sînt soluțiile ecuației (17), unde punem $X_1 = x_1$, $X_2 = x_2$ și $X_3 = x_3$. În acest caz $s_1 = 0$, $s_2 = -p$ și $s_3 = q$. Deci b_1, b_2 sînt rădăcinile ecuației

$$z^2 - 27qz - 27p^3 = 0. \tag{20}$$

Această ecuație se numește *rezolventa* ecuației (16). Din (3), obținem

$$b_1 = -\frac{27q}{2} + 27\sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3},$$

$$b_2 = -\frac{27q}{2} - 27\sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}.$$

Cum $L_{\varepsilon x} = b_1$, atunci $L_{\varepsilon x} = \sqrt[3]{b_1}$ (care are trei valori). Dar $L_{\varepsilon^2 x} \cdot L_{\varepsilon x} = \tau_1^2 - 3\tau_2 = -3p$, deci $L_{\varepsilon^2 x}$ este determinat de $L_{\varepsilon x}$. Înlocuind în relațiile (19), obținem din nou formula lui Cardano de determinare a rădăcinilor ecuației de gradul al treilea (a se vedea § 3).

Prin această metodă rezolvarea ecuației de gradul al treilea (forma redusă) se reduce la rezolvarea ecuației de gradul al doilea [ecuația (17)] și a două ecuații binome de gradul al treilea.

— *Rezolvarea ecuației de gradul al patrulea prin metoda Lagrange.* Considerăm din nou ecuația de gradul al patrulea

$$x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 = 0, \qquad (21)$$

unde a_1, a_2, a_3, a_4 sînt numere complexe. Considerăm polinomul

$$A = X_1 X_2 + X_3 X_4.$$

Am văzut că subgrupul invariant al lui A este

$$H_A = \{e, (1, 2), (3, 4), (1, 2), (3, 4), (1, 3), (2, 4), (1, 4)\ (2, 3), (1, 3, 2, 4), (1, 4, 2, 3)\}$$

care este de indice 3 în σ_4.

Clasele de echivalență la stînga modulo subgrupul H_A sînt

$$\hat{e} = H_A;\quad \widehat{(1, 3)} = (1, 3)\,H_A;\quad \widehat{(1, 4)} = (1, 4)\,H_A.$$

Cele trei valori ale lui A sînt

$$A_1 = A = X_1 X_2 + X_3 X_4,\ A_2 = (1, 3)\,A = X_1 X_4 + X_2 X_3,$$
$$A_3 = (1, 4) = X_1 X_3 + X_2 X_4.$$

Ecuația de gradul al treilea pe care o satisface A este

$$(z - A_1)(z - A_2)(z - A_3) = 0$$

sau

$$z^3 - (A_1 + A_2 + A_3)\,z^2 + (A_1 A_2 + A_1 A_3 + A_2 A_3)\,z - - A_1 A_2 A_3 = 0.$$

Prin calcul rezultă ușor că

$$A_1 + A_2 + A_3 = s_2,$$

$$A_1A_2 + A_1A_3 + A_2A_3 = s_1s_3 - 4s_4,$$

$$A_1A_2A_3 = s_1^2s_4 + s_3^2 - 4s_2s_4.$$

Prin urmare A satisface ecuația

$$z^3 - s_2z^2 + (s_1s_3 - 4s_4)z - (s_1^2s_4 + s_3^2 - 4s_2s_4) = 0. \quad (22)$$

Fie x_1, x_2, x_3, x_4 rădăcinile ecuației (21). Să notăm cu α_i valorile lui A_i $(1 \leqslant i \leqslant 3)$ cînd punem $X_1 = x_1$, $X_2 = x_2$, $X_3 = x_3$ și $X_4 = x_4$. Rezultă din (22) ținînd seama de relațiile lui Viète că α_i $(1 \leqslant i \leqslant 3)$ sînt rădăcinile ecuației

$$z^3 - a_2z^2 + (a_1a_3 - 4a_4)z - (a_1^2a_4 + a_3^2 - 4a_2a_4) = 0. \quad (23)$$

Această ecuație se numește *rezolventa* ecuației inițiale. Dar

$$\left.\begin{aligned} \alpha_1 &= x_1x_2 + x_3x_4 \\ \alpha_2 &= x_1x_4 + x_2x_3 \\ \alpha_3 &= x_1x_3 + x_2x_4 \end{aligned}\right\}. \quad (24)$$

Cum $x_1x_2x_3x_4 = a_4$, din relațiile (24) obținem că x_1x_2 și x_3x_4 sînt soluțiile ecuației

$$z^2 - \alpha_1z + a_4 = 0, \quad (25)$$

x_1x_4 și x_2x_3 sînt soluțiile ecuației

$$z^2 - \alpha_2z + a_4 = 0, \quad (25')$$

iar x_1x_3 și x_2x_4 sînt soluțiile ecuației

$$z^2 - \alpha_3z + a_4 = 0. \quad (25'')$$

Dar este ușor de văzut că odată determinate valorile x_1x_2, x_1x_3, x_2x_3, x_1x_4, ... obținem imediat pe x_1, x_2, x_3 și x_4.

Aşadar, rezolvarea ecuaţiei de gradul al patrulea se reduce la rezolvarea unei ecuaţii de gradul al treilea (rezolventa lui Lagrange) şi a trei ecuaţii de gradul al doilea.

— *Scurt istoric.* Rezolvarea ecuaţiei de gradul doi era cunoscută încă din antichitate. Formula de rezolvare a ecuaţiei de gradul al treilea este cunoscută din perioada renaşterii italiene. Aceasta a fost obţinută prima dată de către Scipione del FERRO (data exactă a descoperirii nu se cunoaşte; se presupune anul 1515). Această formulă a fost regăsită de Niccolo TARTAGLIA (1541). Soluţia lui Tartaglia a fost publicată de Gerolamo CARDANO în *Ars Magna* (1545) şi este cunoscută în general sub denumirea de *formula lui Cardano*. Metoda generală de rezolvare a ecuaţiei de gradul al patrulea care a fost publicată de Cardano în *Ars Magna* este atribuită asistentului lui Cardano, Ludovico FERARRI.

S-a încercat ulterior obţinerea unor formule analoage pentru ecuaţia de gradul al cincilea.

O contribuţie importantă la studiul ecuaţiilor algebrice au avut mari matematicieni ca EULER şi LAGRANGE. LAGRANGE a avut ideea de a reduce rezolvarea ecuaţiei algebrice la un şir de ecuaţii mai simple (numite ecuaţiile rezolvente). În 1813 A. RUFFINI şi apoi independent N. H. ABEL în 1827 au demonstrat că pentru ecuaţiile de grad $n \geqslant 5$ nu pot fi date formule de calcul prin radicali.

În 1830, E. GALOIS a enunţat condiţiile necesare şi suficiente pentru ca o ecuaţie să fie rezolvabilă prin radicali, creînd teoria care este astăzi cunoscută sub denumirea de *teoria lui Galois*, teorie care a determinat întreaga dezvoltare a algebrei sub forma sa modernă.

METODE NUMERICE DE DETERMINARE A RĂDĂCINILOR REALE ALE POLINOAMELOR CU COEFICIENŢI REALI

Se ştie că nu există metode care să permită găsirea expresiilor exacte ale rădăcinilor polinoamelor cu coeficienţi reali, de orice grad. În capitolul al IV-lea am arătat că există formule de rezolvare pentru ecuaţiile de gradul al doilea, al treilea şi al patrulea dar nici acestea de multe ori nu sînt foarte folositoare (mai ales, pentru ecuaţiile de gradul al treilea şi al patrulea). Totuşi diferite probleme de mecanică, fizică, tehnică ş.a. necesită calculul rădăcinilor unor polinoame care adesea au grad superior.

În tehnică de multe ori este suficient, a se cunoaşte valori aproximative ale rădăcinilor cu o precizie dată. Ne propunem ca în acest capitol să indicăm unele metode numerice de determinare aproximativă a rădăcinilor reale ale unui polinom cu coeficienţi reali.

§ 1. Marginile rădăcinilor

Fie f un polinom cu coeficienţi reali. Problema pe care ne-o punem este determinarea marginilor rădăcinilor reale ale lui f.

Din lema 7.1, cap. III, rezultă că dacă

$$f = a_0 + a_1X + \dots + a_nX^n \in \mathbb{C}[X]$$

şi $m = \max(|a_0|, |a_1|, \ldots, |a_{n-1}|)$, atunci oricare ar fi $\alpha \in \mathbb{C}$ astfel încît

$$|\alpha| \geqslant \frac{m}{|a_n|} + 1$$

avem

$$|a_n\alpha^n| > |a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}|$$

şi deci α nu poate fi o rădăcină a lui f.

Aşadar, oricare ar fi $f \in \mathbb{C}[X]$, numărul $\frac{m}{|a_n|} + 1$ este o margine superioară a modulelor rădăcinilor reale şi complexe ale lui f.

În cazul în care se caută margini numai pentru rădăcinile reale ale unui polinom se găsesc unele mai bune. Remarcăm că putem găsi marginile între care pot fi rădăcini, dar acest lucru nu înseamnă că aceste rădăcini trebuie să existe.

Arătăm mai întîi că este suficient să găsim o margine superioară pentru rădăcinile pozitive ale unui polinom.

Într-adevăr, fie un polinom f de grad n şi M_0 o margine superioară a rădăcinilor pozitive ale sale. Considerăm polinoamele

$$g_1(X) = X^n f\left(\frac{1}{X}\right); g_2(X) = f(-X); \; g_3(X) = X^n f\left(-\frac{1}{X}\right)$$

şi fie M_1, M_2, M_3 respectiv, marginile superioare ale rădăcinilor pozitive ale acestor polinoame. Atunci $\frac{1}{M_1}$ este o margine inferioară a rădăcinilor pozitive ale lui f.

Într-adevăr, dacă α este o rădăcină pozitivă a lui f, atunci $\frac{1}{\alpha}$ este o rădăcină pozitivă a lui g_1 şi din inegalitatea $\frac{1}{\alpha} < M_1$ rezultă $\alpha > \frac{1}{M_1}$. De asemenea, se vede uşor că numerele $-M_2$ şi $-\frac{1}{M_3}$ sînt respectiv marginea inferioară şi marginea superioară ale rădăcinilor negative ale polinomului f. Deci, orice

rădăcină pozitivă a lui f este cuprinsă între $\frac{1}{M_1}$ şi M_0, iar orice rădăcină negativă a sa este cuprinsă între $-M_2$ şi $-\frac{1}{M_3}$.

Pentru a găsi o margine superioară a rădăcinilor pozitive procedăm în modul următor. Fie

$$f = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{R}[X]$$

şi să presupunem că $a_n > 0$. Fie a_{n-h} $(h \geqslant 1)$ ultimul coeficient negativ al lui f. Remarcăm că există un astfel de coeficient,, deoarece, în caz contrar, f nu ar avea rădăcini pozitive. Fie de asemenea, M maximul valorilor absolute ale coeficienţilor negativi ai lui f.

Propoziţia 1.1. *Cu notaţiile de mai sus numărul* $\sqrt[h]{\frac{M}{a_n}} + 1$ *este o margine superioară a rădăcinilor pozitive ale polinomului* f.

Demonstraţie. Într-adevăr, fie $\alpha > 1$ astfel că $f(\alpha) = 0$. Atunci

$$a_n\alpha^n \leqslant M \frac{\alpha^{n-h+1} - 1}{\alpha - 1}$$

şi cum $\alpha > 1$, rezultă

$$a_n\alpha^n < M \frac{\alpha^{n-h+1}}{\alpha - 1},$$

adică

$$a_n < \frac{M}{\alpha^{h-1}(\alpha - 1)} < \frac{M}{(\alpha - 1)^h}$$

sau

$$(\alpha - 1)^h < \frac{M}{a_n}.$$

Deci

$$\alpha < \sqrt[h]{\frac{M}{a_n}} + 1,$$

ceea ce trebuia demonstrat.

O altă metodă pentru determinarea marginei superioare a rădăcinilor pozitive este dată de următoarea

Propoziția 1.2 (*Newton*). *Fie* $f = a_0 + a_1X + \ldots + a_nX^n$ *un polinom cu coeficienți reali astfel încît* $a_n > 0$. *Dacă* a *este un număr real pentru care* $f^{(i)}(a) > 0$, *pentru orice* $i = 0, 1, \ldots, n$, *atunci* a *este o margine superioară a rădăcinilor pozitive ale lui* f.

Demonstrație. După formula lui Taylor avem

$$f(X) = f(a) + (X - a)\frac{f'(a)}{1!} + (X - a)^2\frac{f''(a)}{2!} + \ldots$$

$$\ldots + (X - a)^n \frac{f^{(n)}(a)}{n!}.$$

După această formulă rezultă că dacă $x \geqslant a$, atunci $f(x) > 0$ și deci f nu poate avea rădăcini mai mari decît a. Așadar, a este o margine superioară pentru rădăcinile pozitive ale lui f.

Să vedem cum găsim numărul a. Considerăm funcția $x \to f(x)$ de la $\mathbb{R}$ la $\mathbb{R}$. Observăm că $f^{(n)}(x) = n!\, a_n > 0$ și deci $f^{(n-1)}(x)$ este crescătoare. Există deci un număr real b_1 cu $f^{(n-1)}(x) > 0$, pentru $x \geqslant b_1$. Continuînd procedeul, rezultă că $f^{(n-2)}(x)$ este o funcție crescătoare pentru $x \geqslant b_1$. Deci există $b_2 \geqslant b_1$ cu $f^{(n-2)}(x) > 0$ pentru $x \geqslant b_2$. Se va obține în sfîrșit un număr a care îndeplinește condițiile cerute.

Aplicație. Fie polinomul

$$f(X) = X^5 + 7X^4 - 12X^3 - 58X^2 - 52X - 1.$$

Avem $f'(X) = 5X^4 + 28X^3 - 36X^2 - 116X - 52$,

$$\frac{f''(X)}{2!} = 10X^3 + 42X^2 - 36X - 58,$$

$$\frac{f^{(3)}(X)}{3!} = 10X^2 + 28X - 12, \quad \frac{f^{(4)}(X)}{4!} = 5X + 7, \quad \frac{f^{(5)}(X)}{5!} = 1,$$

de unde se vede ușor că

$f^{(4)}(x) > 0$ pentru $x \geqslant 0$,
$f^{(3)}(x) > 0$ pentru $x \geqslant 1$,
$f''(x) > 0$ pentru $x \geqslant 2$,
$f'(x) > 0$ pentru $x \geqslant 3$.

Dar $f(4) > 0$ și atunci o margine superioară a rădăcinilor pozitive ale lui f este $M_0 = 4$.

§ 2. Numărul rădăcinilor reale ale unui polinom cu coeficienți reali

Fie f un polinom de o nedeterminată cu coeficienţi reali. Ne punem problema determinării numărului rădăcinilor reale ale sale. Putem presupune că f nu are rădăcini multiple, deoarece, în caz contrar, considerăm polinomul obţinut prin împărţirea lui f la cel mai mare divizor comun al lui f şi f'. Vom da mai jos una din metodele de determinare a numărului de rădăcini reale ale lui f şi anume *metoda lui Sturm*.

Fie f un polinom cu coeficienţi în $\mathbb{R}$, care nu are rădăcini multiple şi $a < b$ două numere reale. Prin şir Sturm asociat polinomului f pe intervalul $[a, b]$ se înţelege o mulţime ordonată finită de polinoame

$$S = \{f = f_0, f' = f_1, f_2, \ldots, f_t\}$$

care verifică următoarele condiţii:

1° ultimul polinom f_t nu are rădăcini reale;

2° oricare două polinoame consecutive f_i şi f_{i+1}, $0 \leqslant i \leqslant t-1$ nu au rădăcini comune;

3° dacă $x \in \mathbb{R}$ şi $f_i(x) = 0$ pentru un oarecare $i = 1, 2, \ldots$ $\ldots, t-1$, atunci $f_{i-1}(x) f_{i+1}(x) < 0$;

4° avem $f_i(a) \neq 0$ şi $f(b) \neq 0$ pentru $i = 0, 1, \ldots, t$.

Propoziția 2.1. *Pentru orice polinom f din $\mathbb{R}[X]$ care nu are rădăcini multiple există un şir Sturm asociat polinomului f pe intervalul $[a, b]$.*

Demonstrație. Construim şirul cerut prin recurenţă. Fie $f_0 = f$ şi $f_1 = f'$. Dacă $i \geqslant 2$, definim f_i ca fiind opusul restului împărţirii polinomului f_{i-2} la polinomul f_{i-1}. Deci

$$f = f'q_1 - f_2,$$

$$f' = f_2q_2 - f_3,$$

$$\ldots\ldots\ldots\ldots$$

$$f_{i-2} = f_{i-1}q_{i-1} - f_i,$$

$$\ldots\ldots\ldots\ldots$$

Evident, cum gradele lor descresc strict, există doar un număr finit de polinoame f_i obținute în acest mod. Fie f_t ultimul polinom obținut astfel și demonstrăm că

$$\{f_0, f_1, \ldots, f_t\}$$

este un șir Sturm. Cum polinoamele f și f' nu au factori comuni, rezultă că ultimul termen al acestui șir, adică f_t, este o constantă nenulă, deci 1°. Să presupunem că f_{i-1} și f_i au o rădăcină comună. Atunci, din egalitatea

$$f_{i-2} = f_{i-1}\, q_{i-1} - f_i$$

rezultă că f_{i-2} și f_{i-1} au o rădăcină comună. Continuînd procesul, rezultă că f și f' au o rădăcină comună, ceea ce reprezintă o contradicție. Deci condiția 2° este satisfăcută. Fie acum x o rădăcină reală a polinomului f_i, $1 \leqslant i \leqslant t-1$. Din relația $f_{i-1} = f_i q_i - f_{i-1}$ rezultă $f_{i-1}(x) = -f_{i+1}(x)$ și deci $f_{i-1}(x)\, f_{i+1}(x) = -(f_{i+1}(x))^2 < 0$.

Dacă $S = \{f, f_1, \ldots, f_t\}$ este un șir Sturm, pentru orice element x din $[a, b]$ care nu este o rădăcină a nici unuia din polinoamele f_i, vom nota prin $W_S(x)$ numărul variațiilor de semn în șirul

$$f(x), f_1(x), \ldots, f_t(x)$$

și vom numi $W_S(x)$ *variația semnelor* în acest șir.

Teorema 2.2 (*Sturm*). *Fie f un polinom din* $\mathbb{R}[X]$ *care nu are rădăcini multiple. Atunci numărul rădăcinilor reale ale polinomului f cuprinse între două numere reale a și b este egal cu diferența $W_S(b) - W_S(a)$, pentru orice șir Sturm S.*

Demonstrație. Fie $x_1, x_2, \ldots, x_r$ rădăcinile reale ale polinoamelor f_i în $[a, b]$, pentru $i = 0, 1, \ldots, t-1$, și să presupunem că $x_1 < x_2 < \ldots < x_r$. Atunci variația $W_s(x)$ rămîne constantă în intervalele deschise cuprinse între aceste rădăcini.

Într-adevăr, să presupunem că pe un anumit interval (x_k, x_{k+1}) variația $W_s(x)$ nu este constantă. Aceasta înseamnă că există $\alpha, \beta \in (x_k, x_{k+1})$ astfel încît pentru un i avem $f_i(\alpha) f_i(\beta) < 0$. Dar atunci, cum evident funcția $x \to f_i(x)$ de la $\mathbb{R}$ la $\mathbb{R}$ este continuă, există $c \in (\alpha, \beta)$, astfel încît $f_i(c) = 0$. Însă c fiind

diferit de $x_1, x_2, \ldots, x_r$, a apărut o contradicţie. Prin urmare, este suficient să demonstrăm că dacă avem un y real (şi numai unul) astfel că $a < y < b$ şi y este o rădăcină a unui polinom oarecare f_i, atunci diferenţa $W_s(a) - W_s(b)$ este egală cu 1 cînd y este o rădăcină a lui f şi cu 0 în caz contrar. Să presupunem, mai întîi, că $f_i(y) = 0$ pentru un anumit $1 \leqslant i \leqslant t-1$. Atunci, după 3° rezultă că $f_{i-1}(y)$ şi $f_{i+1}(y)$ au semne contrare iar aceste semne nu se schimbă dacă înlocuim pe y prin a sau b. Deci variaţiile semnelor în şirurile

$$f_{i-1}(a), f_i(a), f_{i+1}(a) \text{ şi } f_{i-1}(b), f_i(b), f_{i+1}(b)$$

sînt egale şi anume egale cu 1. Astfel am arătat că dacă y nu este rădăcină a lui f, atunci $W_s(a) = W_s(b)$. Dacă y este o rădăcină a lui f, atunci $f(a)$ şi $f(b)$ au semne contrare, iar $f'(a)$ şi $f'(b)$ au ambele acelaşi semn cu $f(b)$. Prin urmare, $W_s(a) = W_s(b) + 1$ sau $W_s(a) - W_s(b) = 1$ şi teorema este demonstrată.

Pentru a obţine numărul tuturor rădăcinilor reale ale lui f, este suficient să aplicăm această teoremă la intervalul $(-\infty, +\infty)$, iar pentru a obţine numărul rădăcinilor pozitive (respectiv negative) ale lui f, aplicăm teorema la intervalul $(0, +\infty)$ [respectiv $(-\infty, 0)$].

Aplicaţii. 1. Determinarea numărului rădăcinilor reale ale unui polinom de gradul al treilea, $f = X^3 + pX + q$, cu coeficienţi reali. Şirul său Sturm este

$$f_0 = f,\ f_1 = 3X^2 + p,\ f_2 = -2pX - 3q,\ f_3 = -4p^3 - 27q^2.$$

Dacă $-4p^3 - 27q^2 \geqslant 0$, atunci $p \leqslant 0$. Toţi coeficienţii termenilor de grad maxim sînt pozitivi şi, prin urmare, $W_s(-\infty) - W_s(+\infty) = 3$, deci f are trei rădăcini reale.

Dacă $-4p^3 - 27q^2 < 0$, atunci $W_s(-\infty) = 2$ şi $W_s(+\infty) = 1$, deci $W_s(-\infty) - W_s(+\infty) = 1$ şi, prin urmare, polinomul f are o singură rădăcină reală.

2. Cu teorema lui Sturm putem găsi de asemenea şi intervalele în care se găsesc rădăcinile reale ale unui polinom. De exemplu, fie polinomul $f = X^3 + X^2 - 2X - 1$. Şirul lui Sturm este

$$f_0 = f,\ f_1 = 3X^2 + 2X - 2,\ f_2 = 2X + 1,\ f_3 = 1.$$

	f	f_1	f_2	f_3	Numărul schimbărilor de semn
$-\infty$	$-$	$+$	$-$	$+$	3
$+\infty$	$+$	$+$	$+$	$+$	0

Rezultă că $W_s(-\infty) - W_s(+\infty) = 3$, deci polinomul f are trei rădăcini reale. Putem găsi și intervalele unde se găsesc aceste rădăcini și anume $(-2, -1)$, $(-1, 0)$, $(1, 2)$. Într-adevăr, avem următorul tabel:

	f	f_1	f_2	f_3	Numărul schimbărilor de semn
-2	$-$	$+$	$-$	$+$	3
-1	$+$	$-$	$-$	$+$	2
0	$-$	$-$	$+$	$+$	1
1	$-$	$+$	$+$	$+$	1
2	$+$	$+$	$+$	$+$	0

Observație. Metoda dată de teorema lui Sturm are unele inconveniente care țin de găsirea șirului Sturm asociat. Există și alte teoreme ca teorema lui Descartes, teorema lui Fourier care limitează superior numărul de rădăcini reale ale unui polinom, dar nu dă numărul exact al lor.

§ 3. Aproximarea rădăcinilor reale ale unui polinom

Pentru a calcula cu aproximație rădăcinile reale ale unui polinom cu coeficienți reali trebuie mai întîi să separăm rădăcinile reale ale lui f, adică să găsim intervale distincte (a_k, b_k) astfel încît fiecare dintre acestea să conțină o singură rădăcină reală x_k a lui f. Am văzut pe un exemplu (vezi aplicația 2) cum se aplică teorema lui Sturm la separarea rădăcinilor reale. Un alt rezultat bine cunoscut și care se poate folosi în acest sens este o consecință a teoremei lui Rolle, care spune că între două rădăcini consecutive ale derivatei unui polinom f cu coeficienți reali există cel mult o rădăcină a lui f. Dacă intervalul (a, b) în care se găsește rădăcina x_0 a unui polinom f este suficient de mic, se poate lua ca valoare aproximativă a acestei rădăcini orice număr din acest interval.

A aproxima rădăcina x_0 cu o eroare mai mică decît 10^{-n} înseamnă a determina un interval (a, b) cu $a < x_0 < b$ și $0 < b - a < 10^{-n}$. Există mai multe metode de a calcula repede și cu o precizie dată valorile aproximative ale rădăcinilor unui polinom. Vom da două din acestea.

În continuare vom presupune f un polinom cu coeficienţi reali şi x_0 o rădăcină simplă a lui f (am observat mai înainte că putem face tot timpul această presupunere). Mai mult, fie (a, b) un interval cu a şi b raţionali astfel că $a < x_0 < b$ şi x_0 este singura rădăcină a lui f în acest interval. Deci $f(a)$ şi $f(b)$ au semne contrare.

Din ipoteza că x_0 este rădăcină simplă a lui f rezultă $f'(x_0) \neq \neq 0$. Putem presupune şi că $f''(x_0) \neq 0$, deoarece, în caz contrar, reducem problema la polinomul f'' care este de grad strict mai mic decît gradul lui f.

Fie funcţia $x \to f(x)$ definită pe $\mathbb{R}$ cu valori în $\mathbb{R}$. Rezultă că există doar următoarele patru posibilităţi reprezentate grafic în plan, pentru fiecare caz în parte în figurile 7—10 :

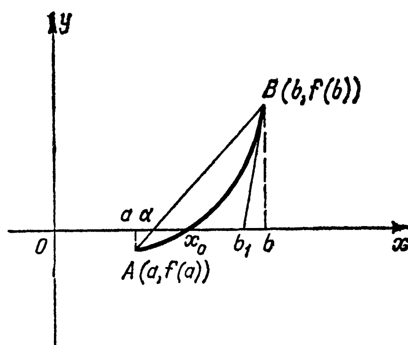


Fig. 7

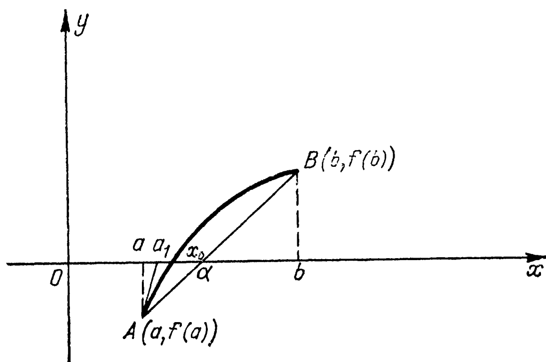


Fig. 8

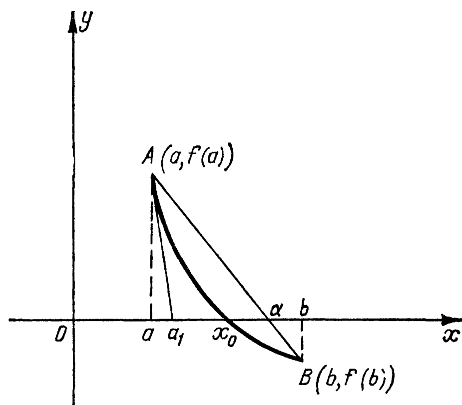


Fig. 9

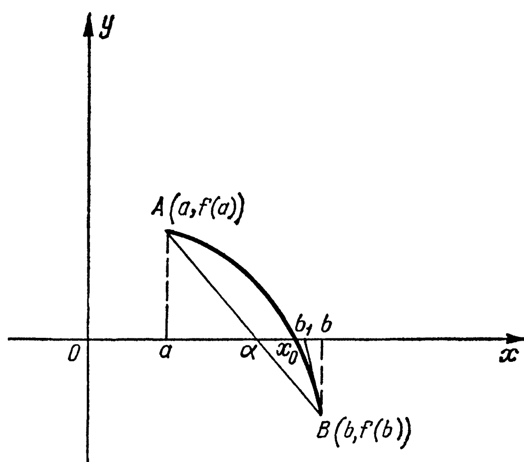


Fig. 10

1. $f'(x) > 0$, $f''(x) > 0$, pentru orice $x \in [a, b]$;
2. $f'(x) > 0$, $f''(x) < 0$, pentru orice $x \in [a, b]$;
3. $f'(x) < 0$, $f''(x) > 0$ pentru orice $x \in [a, b]$;
4. $f'(x) < 0$, $f''(x) < 0$, pentru orice $x \in [a, b]$.

Metoda interpolării liniare (*metoda coardei*). Această metodă constă în a lua ca valoare aproximativă a rădăcinii x_0 un

număr α care împarte intervalul (a, b) în două părţi ale căror lungimi sînt proporţionale cu valorile absolute ale numerelor $f(a)$ şi $(f(b)$, adică

$$\frac{\alpha - a}{b - \alpha} = -\frac{f(a)}{f(b)} .$$

Deci

$$\alpha = \frac{bf(a) - af(b)}{f(a) - f(b)} .$$

Din punct de vedere geometric metoda interpolării liniare constă în înlocuirea, în intervalul (a, b), a curbei $y = f(x)$ prin coarda care uneşte punctele $A(a, f(a))$ şi $B(b, f(b))$ şi se ia ca valoare aproximativă a lui x_0 abscisa α a punctului de intersecţie a acestei coarde cu axa absciselor.

— *Metoda lui Newton.* Considerăm extremitatea intervalului (a, b) în care $f(x)$ şi $f''(x)$ au acelaşi semn (una din ele îndeplineşte cu siguranţă această condiţie). Astfel, pentru cazurile 2 şi 3 (fig. 8 şi fig. 9) aceasta este a iar pentru cazurile 1 şi 4 (fig. 7 şi fig. 10) este b. Ducem tangenta la curba $y = f(x)$ în punctul de coordonate $(a, f(a))$ sau $(b, f(b))$ după cum am ales extremitatea a sau b a intervalului. Fie β abscisa punctului de intersecţie al acestei tangente cu axa Ox. Se ia ca valoare aproximativă a lui x_0 numărul β. Deci metoda lui Newton constă în înlocuirea, în intervalul (a, b), a curbei $y = f(x)$ printr-o tangentă la această curbă trecînd printr-unul din punctele $(a, f(a))$ sau $(b, f(b))$, după caz.

Remarcăm că este foarte important să ducem tangenta în extremitatea aleasă; altfel, ne putem depărta foarte mult de x_0. Să găsim formula care dă pe β. Ecuaţia tangentei într-un punct $(\gamma, f(\gamma))$ al curbei $y = f(x)$ este

$$y - f(\gamma) = f'(\gamma)\,(x - \gamma).$$

Atunci abscisa β a punctului de intersecţie al acestei tangente cu axa Ox se obţine din

$$-f(\gamma) = f'(\gamma)\,(\beta - \gamma),$$

de unde

$$\beta = \gamma - \frac{f(\gamma)}{f'(\gamma)} .$$

În cazurile 2 și 3 se obține $\gamma = a$ și deci

$$\beta = a - \frac{f(a)}{f'(a)} ,$$

iar în cazurile 1 și 4 se obține $\gamma = b$ și deci

$$\beta = b - \frac{f(b)}{f'(b)} .$$

Să arătăm că β este o valoare aproximativă a rădăcinii x_0, mai bună decît extremitățile intervalului (a, b). Fie $x_0 = \gamma + h_0$, unde $h_0 > 0$ dacă $\gamma = a$ și $h_0 < 0$ dacă $\gamma = b$. Avem

$$\beta = \gamma - \frac{f(\gamma)}{f'(\gamma)} = \gamma + h, \text{ unde } h = - \frac{f(\gamma)}{f'(\gamma)} .$$

Pentru ca β să fie o valoare aproximativă a lui x_0 mai bună decît γ, trebuie să fie satisfăcute condițiile :

1° Dacă $\gamma = a$, atunci $\gamma < \beta < x_0$.

2° Dacă $\gamma = b$, atunci $\gamma > \beta > x_0$.

De aici rezultă, înlocuind $x_0 = \gamma + h_0$ și $\beta = \gamma + h$, că în ambele cazuri trebuie să avem $h(h - h_0) < 0$. Să evaluăm pe $h - h_0$.

După formula lui Taylor obținem :

$$0 = f(x_0) = f(\gamma + h_0) = f(\gamma) + h_0 f'(\gamma) + \frac{h_0^2}{2!} f''(\gamma + \theta h_0),$$

unde $0 < \theta < 1$. Dar $f(\gamma) + hf'(\gamma) = 0$, de unde

$$h - h_0 = \frac{h_0^2}{2!} \cdot \frac{f''(\gamma + \theta h_0)}{f'(\gamma)} .$$

Deci $h(h - h_0) = -\frac{h_0^2}{2!} \cdot \frac{f(\gamma) f''(\gamma + \theta h_0)}{[f'(\gamma)]^2}$. Deoarece $f''(x)$ are semn constant în (a, b), rezultă că $f''(\gamma + \theta h_0)$ şi $f''(\gamma)$ au acelaşi semn. Deci dacă $f''(\gamma) f(\gamma) > 0$, atunci $h(h - h_0) < 0$. Aşadar, dacă γ este extremitatea intervalului în care $f''(\gamma)\ f(\gamma) > 0$, atunci β dat de metoda lui Newton este o valoare aproximativă a lui x_0 mai bună decît extremităţile intervalului.

Observăm că metoda interpolării liniare şi metoda lui Newton dau valori aproximative pentru x_0, anume α şi respectiv β, care încadrează pe x_0. Astfel, dacă condiţiile problemei ne permit, este bine să folosim alternativ cele două metode pentru găsirea unei aproximaţii a lui x_0 cît de bună dorim.

Vom arăta că metoda lui Newton foloseşte la calcularea valorii unei rădăcini cu orice eroare dorim.

Fie x_0 o rădăcină simplă a lui f care se găseşte în intervalul (a, b). Mai mult, presupunem că sînt verificate condiţiile din metoda lui Newton pentru acest interval. Deci există numerele pozitive A şi B astfel încît pe (a, b) să avem

$$|f'(x)| > A,\ |f''(x)| < B.$$

Fie $C = \frac{B}{2A}$ şi, eventual restrîngînd intervalul (a, b), ceea ce nu afectează inegalităţile precedente, putem presupune că

$$C(b - a) < 1.$$

Fie $\gamma = \beta_0$ capătul intervalului (a, b) pentru care începem să aplicăm metoda lui Newton. După această metodă, aplicată succesiv, se obţine un şir $\beta_1, \beta_2, \ldots, \beta_k, \ldots$ de valori aproximative ale rădăcinii x_0. Avem $a < \beta_i < b$, oricare ar fi $i = 1, 2, \ldots$ $\ldots, k, \ldots$ şi

$$\beta_k = \beta_{k-1} - \frac{f(\beta_{k-1})}{f'(\beta_{k-1})},\ k = 1, 2, \ldots$$

Fie $x_0 = \beta_k + h_k$, $k = 0, 1, 2, \ldots$ Atunci

$$0 = f(x_0) = f(\beta_k + h_k) = f(\beta_k) + h_k f'(\beta_k) + \frac{h_k^2}{2!} f''(\beta_k + \theta h_k),$$

unde $0 < \theta < 1$. Cum $f'(\beta_k) \neq 0$, atunci se obţine

$$-\frac{h_k^2}{2!}\frac{f''(\beta_k + \theta h_k)}{f'(\beta_k)} = h_k + \frac{f(\beta_k)}{f'(\beta_k)} = x_0 - \left(\beta_k - \frac{f(\beta_k)}{f'(\beta_k)}\right) =$$

$$= \alpha - \beta_{k+1} = h_{k+1}.$$

Atunci

$$|h_{k+1}| = h_k^2 \left|\frac{f''(\beta_k + \theta h_k)}{2f'(\beta_k)}\right| < h_k^2 \frac{B}{2A} = Ch_k^2, \quad k = 0, 1, 2, \ldots$$

şi deci

$$|h_{k+1}| < Ch_k^2 < C^3 h_{k-1}^4 < C^7 h_{k-2}^8 < \ldots < C^{2^{k+1}} - 1\, h_0^{2^{k+1}}$$

sau încă, deoarece $|h_0| < |b - a|$, atunci

$$|h_{k+1}| < C^{-1}|C(b - a)|^{2^{k+1}}, \quad k = 0, 1, 2, \ldots$$

Aşadar, cînd k tinde către infinit, diferenţa h_k dintre rădăcina x_0 şi valoarea sa aproximativă β_k, obţinută prin aplicarea succesivă a metodei lui Newton, tinde către zero. Acest fapt demonstrează convergenţa metodei lui Newton. De asemenea, ultima formulă dă o estimare a erorii făcute la a $(k + 1) - a$ iteraţie a metodei lui Newton.

Aplicaţie. Să se calculeze cu aproximaţie de 0,0001 rădăcinile reale ale polinomului

$$f(x) = x^3 - 2x - 5.$$

După metoda lui Newton (propoziţia 1.2) se găseşte că o margine superioară a rădăcinilor reale pozitive ale lui f este $M_0 = 3$. De asemenea, se vede că polinomul are o singură rădăcină reală x_0 cuprinsă în intervalul (2, 3). Să micşorăm şi mai mult intervalul în care se află rădăcina. Avînd $f(2,1) = 0{,}061 > 0$, iar $f(2{,}09) = -0{,}050671 < 0$, rezultă

$$2{,}09 < x_0 < 2{,}1.$$

Cum $f''(x) = 6x > 0$ pentru $x \in [2{,}09 ; 2{,}1]$, rădăcina se găseşte în intervalul determinat de abscisele punctelor de intersecţie cu axa Ox a coardei AB şi a tangentei la curbă în punctul B. Punctul B va fi cel ales deoarece $f''(2,1)\,f(2,1) > 0$,

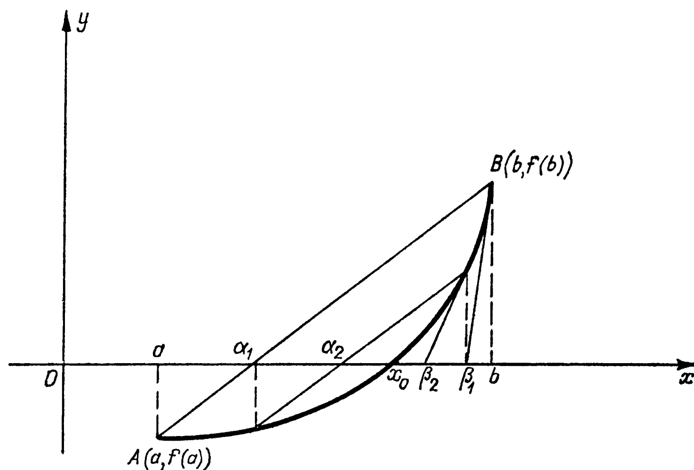


Fig. 11

$$A(2{,}09;\ -0{,}050671) \text{ și } B(2{,}1;\ 0{,}061).$$

Avem

$$\alpha_1 = a - \frac{(b-a)\,f(a)}{f(b)-f(a)} = 2{,}09 - \frac{(2{,}10-2{,}09)\,f(2{,}09)}{f(2{,}1)-f(2{,}09)} =$$

$$= 2{,}09 - \frac{0{,}01\cdot(-0{,}050671)}{0{,}061+0{,}050671} \approx 2{,}09453,$$

$$\beta_1 = b - \frac{f(b)}{f'(b)} = 2{,}1 - \frac{f(2{,}1)}{f'(2{,}1)} = 2{,}1 - \frac{0{,}061}{11{,}23} \approx 2{,}09457.$$

Deci

$$2{,}09453 < x_0 < 2{,}09457.$$

Valoarea aproximativă a lui x_0 cu patru zecimale exacte este 2,0945.

VI

ELEMENTE DE TEORIA CORPURILOR

În tot acest capitol corpurile cu care vom lucra sînt subcorpuri ale corpului numerelor complexe. Orice astfel de corp conține corpul numerelor raționale $\mathbb{Q}$.

§ 1. Extinderi finite

Dacă K și E sînt două corpuri astfel încît K este un subcorp al lui E, se spune că E este o *extindere* a lui K și se notează prin $K \subset E$. În particular, rezultă că orice corp este o extindere a corpului $\mathbb{Q}$. O extindere E a corpului K se numește *finită* dacă există în corpul E un număr finit de elemente $\alpha_1, \alpha_2, \ldots, \alpha_n$, astfel încît orice element $\beta \in E$ se scrie în mod unic sub forma unei combinații liniare de aceste elemente cu coeficienți în corpul K:

$$\beta = a_1\alpha_1 + \ldots + a_n\alpha_n, \quad a_1, a_2, \ldots, a_n \in K.$$

Un sistem de elemente $\alpha_1, \ldots, \alpha_n$ care are această proprietate se numește *bază* a extinderii E peste corpul K. Se vede ușor că sistemul de elemente $\alpha_1, \ldots, \alpha_n$ este o bază a lui E peste K dacă:

1) Pentru orice $\beta \in E$ există $a_1, a_2, \ldots, a_n$ din K astfel încît $\beta = \sum_{i=1}^{n} a_i \alpha_i$ (se zice că $\alpha_1, \alpha_2, \ldots, \alpha_n$ generează liniar extinderea E peste corpul K).

2) Din egalitatea $\sum_{i=1}^{n} a_i \alpha_i = 0$ cu $a_1, a_2, \ldots, a_n \in K$ rezultă că $a_i = 0$ $(1 \leqslant i \leqslant n)$ (se spune că $\alpha_1, \ldots, \alpha_n$ sînt liniar independente peste K).

Propoziția 1.1. *Fie E o extindere a corpului K și $\alpha_1, \alpha_2, \ldots, \alpha_n$ o bază a lui E peste K. Dacă $\beta_1, \beta_2, \ldots, \beta_m$ sînt elemente din E astfel încît $m > n$, atunci există $b_1, b_2, \ldots, b_m \in K$, nu toate nule, astfel încît*

$$b_1\beta_1 + \ldots + b_m\beta_m = 0.$$

În particular, rezultă că două baze ale lui E peste K au același număr de elemente.

Demonstrație. Cum $\alpha_1, \alpha_2, \ldots, \alpha_n$ este o bază a lui E peste K, atunci fiecare β_i se poate scrie sub forma

$$\beta_i = \sum_{j=1}^{n} a_{ij}\, \alpha_j, \text{ unde } a_{ij} \in K.$$

În felul acesta obținem sistemul de m ecuații cu n necunoscute

$$\sum_{j=1}^{n} a_{ij}\, x_j = \beta_i, \qquad 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n, \tag{1}$$

care admite ca soluție nenulă pe $x_1 = \alpha_1, \ldots, x_n = \alpha_n$. Fie matricele

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \text{ și } B = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} & \beta_1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & \beta_m \end{pmatrix}.$$

Întrucît sistemul (1) este compatibil, rangul matricei A este egal cu rangul matricei B. Fie rang$A = r$. Dacă $m > n$, atunci $r \leqslant n$. Putem presupune fără a micșora generalitatea că submatricea

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1r} \\ a_{21} & a_{22} & \ldots & a_{2r} \\ \ldots & \ldots & \ldots & \ldots \\ a_{r1} & a_{r2} & \ldots & a_{rr} \end{pmatrix}$$

are determinantul nenul. Rezultă că

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1r} & \beta_1 \\ a_{21} & a_{22} & \dots & a_{2r} & \beta_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{r1} & a_{r2} & \dots & a_{rr} & \beta_r \\ a_{r+11} & a_{r+12} & \dots & a_{r+1r} & \beta_{r+1} \end{vmatrix} = 0,$$

care, dezvoltat după ultima coloană, ne dă că există numerele $b_1, b_2, \dots, b_{r+1} \in K$, unde b_{r+1} este determinantul matricei

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \cdot & \cdot & \cdot & \cdot \\ a_{r1} & a_{r2} & \dots & a_{rr} \end{pmatrix},$$

pentru care $b_1\beta_1 + b_2\beta_2 + \dots + b_{r+1}\beta_{r+1} = 0$ ($b_{r+1} \neq 0$). Se poate scrie

$$b_1\beta_1 + b_2\beta_2 + \dots + b_m\beta_m = 0,$$

unde $b_i = 0$ pentru $i \geqslant r + 2$.

Propoziţia precedentă permite să definim gradul extinderii E peste K, ca fiind numărul elementelor dintr-o bază arbitrară a lui E peste K. Acest număr se notează $[E : K]$.

Observaţii. 1. $[E : K] = 1$ dacă şi numai dacă $E = K$. Într-adevăr, dacă $E = K$, atunci $[E : K] = 1$, deoarece 1 este o bază a extinderii E peste K. Reciproc, dacă $[E : K] = 1$, fie $\{\alpha\}$ o bază a lui E peste K. Atunci există un $a \in K$ astfel încît $1 = a\alpha$. Deci $\alpha = a^{-1}$, de unde rezultă că $\alpha \in K$. Se vede uşor că $E \subset K$ şi deci $E = K$.

2. Dacă E este o extindere finită a lui K, $[E : K]$ este egal cu dimensiunea lui E peste K considerat ca spaţiu vectorial.

Propoziţia 1.2. *Fie E o extindere finită a lui K şi F o extindere finită a lui E. Atunci F este o extindere finită a lui K şi în plus are loc egalitatea*

$$[F : K] = [F : E]\,[E : K].$$

Demonstraţie. Fie $\alpha_1, \alpha_2, \dots, \alpha_n$ o bază a lui E peste K şi $\beta_1, \beta_2, \dots, \beta_m$ o bază a lui F peste E. Este suficient să do-

vedim că sistemul de elemente $\{\alpha_i \, \beta_j\}_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$ este o bază a lui F pe K. Fie $z \in F$; există $b_1, b_2, \ldots, b_m$, elemente din E, astfel încît

$$z = b_1\beta_1 + \ldots + b_m \beta_m = \sum_{k=1}^{m} b_k \beta_k.$$

Pentru fiecare $b_i \in E$ există elemente $a_{i1}, \ldots, a_{in}$ din K astfel încît

$$b_i = \sum_{s=1}^{n} a_{is} \alpha_s.$$

Atunci

$$z = \sum_{i=1}^{m} b_i \beta_i = \sum_{i=1}^{m} \left(\sum_{s=1}^{n} a_{is} \alpha_s \right) \beta_i = \sum_{i,s=1}^{m,n} a_{is} \alpha_s \beta_i.$$

Se demonstrează că $\{\alpha_i \, \beta_j\}_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$ sînt liniar independenţi peste K. Fie egalitatea

$$\sum_{i,j=1}^{n,m} a_{ij} \alpha_i \beta_j = 0 \text{ cu } a_{ij} \in K \, (1 \leqslant i \leqslant n, \quad 1 \leqslant j \leqslant m).$$

Această egalitate se poate scrie

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} \alpha_i \right) \beta_j = 0.$$

Cum $\beta_1, \ldots, \beta_m$ este o bază a lui F peste E, se obţine

$$\sum_{i=1}^{n} a_{ij} \alpha_i = 0 \quad (1 \leqslant j \leqslant m)$$

şi deoarece $\alpha_1, \alpha_2, \ldots, \alpha_n$ este o bază a lui E peste K, rezultă $a_{ij} = 0$ pentru orice $1 \leqslant i \leqslant n$ şi $1 \leqslant j \leqslant m$.

§ 2. Extinderi finit generate

Fie K un corp (adică un subcorp al numerelor complexe) şi $\alpha_1, \alpha_2, \ldots, \alpha_n$ numere complexe arbitrare. Să considerăm toate

corpurile care sînt extinderi ale lui K şi care conţin numerele $\alpha_1, \alpha_2, \ldots, \alpha_n$. Astfel de corpuri există, deoarece, de exemplu, printre acestea se află corpul $\mathbb{C}$ al numerelor complexe. Se vede uşor că intersecţia tuturor acestor corpuri este de asemenea un corp şi este, desigur, cea mai mică extindere a lui K ce conţine numerele $\alpha_1, \alpha_2, \ldots, \alpha_n$; se notează cu $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ şi se numeşte *extinderea generată de numerele* $\alpha_1, \alpha_2, \ldots, \alpha_n$.

O extindere E a lui K se spune *finit generată* dacă există elementele $\alpha_1, \alpha_2, \ldots, \alpha_n$ astfel încît $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Este uşor de verificat că:

1) $K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K$ dacă şi numai dacă $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$;

2) $K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_i)(\alpha_{i+1}, \ldots, \alpha_n)$ pentru orice $1 \leqslant i \leqslant n$;

3) Dacă E este o extindere finită a lui K cu baza $\alpha_1, \alpha_2, \ldots, \alpha_n$, atunci $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, adică este finit generată.

Notăm

$$K[\alpha_1, \alpha_2, \ldots, \alpha_n] = \{x \in \mathbb{C} \mid \text{există } f \in K[X_1, \ldots, X_n],\ x = f(\alpha_1, \ldots, \alpha_n)\}.$$

Se vede uşor că $K[\alpha_1, \alpha_2, \ldots, \alpha_n]$ este un subinel al lui $\mathbb{C}$ şi este cel mai mic subinel al lui $\mathbb{C}$ care conţine corpul K şi elementele

$$\alpha_1, \alpha_2, \ldots, \alpha_n \text{ şi că } K[\alpha_1, \alpha_2, \ldots, \alpha_n] \subseteq K(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

§ 3. Elemente algebrice. Extinderi algebrice

Fie K un corp. Un număr complex α se zice *algebric* peste K dacă există un polinom nenul $f \in K[X]$ astfel încît $f(\alpha) = 0$.

Un număr complex α care nu este algebric peste K se numeşte *transcendent* peste corpul K.

Un număr complex α care este algebric (respectiv transcendent) peste corpul numerelor raţionale $\mathbb{Q}$ se numeşte, simplu, *număr algebric* (respectiv *număr transcendent*).

Dacă α este algebric peste K, putem alege un polinom unitar nenul $f \in K[X]$ de cel mai mic grad astfel încît $f(\alpha) = 0$. Un astfel de polinom se numeşte *polinomul minimal* al lui α.

Fie $g \in K[X]$ un alt polinom astfel încît $g(\alpha) = 0$. Din formula împărţirii cu rest există polinoamele $q, r \in K[X]$ astfel încît

$$g = fq + r \text{ cu grad } r < \text{grad } f.$$

Făcînd $X = \alpha$, obținem $r(\alpha) = 0$. Dar cum f este polinomul minimal al lui α, atunci $r = 0$. Rezultă deci că f divide pe g.

În particular, rezultă că polinomul minimal al lui α este unic determinat. Polinomul minimal este ireductibil. Într-adevăr, dacă $f = f_1 \cdot f_2$ cu grad $f_1 <$ grad f și grad $f_2 <$ grad$f$, atunci $0 = f(\alpha) = f_1(\alpha) \cdot f_2(\alpha)$. Deci $f_1(\alpha) = 0$ sau $f_2(\alpha) = 0$, ceea ce contrazice minimalitatea lui f. Din faptul că f este ireductibil rezultă că toate rădăcinile lui f (în corpul $\mathbb{C}$) sînt distincte între ele (vezi cap. III, propoziția 4.6).

O extindere E a lui K se numește *algebrică* dacă orice element al lui E este algebric peste K.

Exemplu. 1. Numărul $\sqrt{2}$ este algebric peste corpul $\mathbb{Q}$, deoarece este rădăcina polinomului $X^2 - 2 \in \mathbb{Q}[X]$ care este și polinomul său minimal.

2. Numărul $\sqrt{2} + \sqrt{3}$ este algebric peste corpul $\mathbb{Q}$, deoarece este rădăcina polinomului $X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$ care este și polinomul său minimal.

3. Corpul numerelor complexe $\mathbb{C}$ este o extindere algebrică a corpului numerelor reale $\mathbb{R}$. Într-adevăr, dacă $z = a + ib$ este un număr complex, atunci z este rădăcina polinomului

$$X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X].$$

4. Numerele reale e, π sînt transcendente peste corpul numerelor raționale,

Propoziția 3.1. *Dacă E este* o *extindere finită a lui K, atunci E este algebrică peste K.*

Demonstrație. Să presupunem că $n = [E:K]$ și fie $\alpha \in E$. Considerăm elementele $1, \alpha, \alpha^2, \ldots, \alpha^n$ care sînt în număr de $n + 1$. Aplicînd propoziția 1.1, există $a_0, a_1, \ldots, a_n \in K$, nu toate nule, astfel încît $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$. Polinomul $f = a_0 + a_1X + \ldots + a_n X^n$ aparține lui $K[X]$ și este nenul. Cum $f(\alpha) = 0$, înseamnă că α este algebric peste K.

Propoziția 3.2. *Fie K un corp și α un număr complex algebric peste K. Atunci $K(\alpha)$ este o extindere finită a lui K și $[K(\alpha):K]$ este egal cu gradul polinomului minimal al lui α. În plus, $K(\alpha) = K[\alpha]$, unde $K[\alpha] = \{g(\alpha) | g \in K[X]\}$.*

Demonstrație. Fie f polinomul minimal al lui α și $n =$ grad f. Vom dovedi egalitatea $K(\alpha) = K[\alpha]$. Este clar că $K[\alpha] \subseteq K(\alpha)$. Egalitatea rezultă dacă dovedim că $K[\alpha]$ este un corp.

Se vede ușor că $K[\alpha]$ este un subinel al lui $\mathbb{C}$. Fie acum $x \in K[\alpha]$, $x \neq 0$. Scriem $x = g(\alpha)$ cu $g \in K[X]$. După formula împărțirii cu rest a lui g prin f:

$$g = fq + r \text{ cu grad } r < n,$$

rezultă

$$x = g(\alpha) = f(\alpha)\, q(\alpha) + r(\alpha) = r(\alpha).$$

Cum grad $r < n$ şi f este ireductibil, atunci polinoamele f şi r sînt prime între ele. Deci, există $u, v \in K[X]$ astfel încît $1 = fu + rv$. Făcînd $X = \alpha$, obţinem

$$1 = f(\alpha)\, u(\alpha) + r(\alpha)\, v(\alpha) = r(\alpha)\, v(\alpha) = v(\alpha)x.$$

Întrucît $v(\alpha) = K[\alpha]$, rezultă că x este inversabil în $K[\alpha]$ şi deci $K[\alpha]$ este un corp. Dar $\alpha \in K[\alpha]$ şi deci $K[\alpha] = K(\alpha)$.

Vom arăta că $1, \alpha, \ldots, \alpha^{n-1}$ formează o bază pentru $K(\alpha) = K[\alpha]$. De mai sus rezultă că dacă $x \in K[\alpha]$, atunci există $r \in K[X]$ astfel încît $x = r(\alpha)$ şi grad $r \leqslant n - 1$. Mai rămîne de verificat că $1, \alpha, \ldots, \alpha^{n-1}$ sînt liniar independente peste K. Fie $a_0, a_1, \ldots, a_{n-1} \in K$ astfel încît

$$a_0 + a_1\alpha + \ldots + a_{n-1}\, \alpha^{n-1} = 0$$

şi polinomul $h = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} \in K[X]$. Deoarece $h(\alpha) = 0$ şi grad $(h) <$ grad (f), rezultă $h = 0$ şi deci $a_0 = a_1 = \ldots = a_{n-1} = 0$.

Corolarul 3.3. *Fie $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ şi $\alpha_1, \alpha_2, \ldots, \alpha_n$ algebrice peste K. Atunci E este o extindere finită a lui K. În plus,*

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K[\alpha_1, \alpha_2, \ldots, \alpha_n].$$

Demonstraţie. Demonstrăm prin inducţie după n. Dacă $n = 1$, aplicăm propoziţia 3.2. Presupunem afirmaţia adevărată pentru $n - 1$ şi să arătăm că este adevărată pentru n. Din ipoteza de inducţie rezultă că $K(\alpha_1, \ldots, \alpha_{n-1})$ este o extindere finită a lui K. Întrucît α este algebric peste K, atunci el este algebric şi peste $K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$. Deci $K(\alpha_1, \ldots, \alpha_n)$ este o extindere finită a lui $K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$. În continuare, aplicăm propoziţia 1.2.

Corolarul 3.4. *Dacă E este o extindere algebrică şi finit generată a lui K, atunci E este o extindere finită a lui K.*

Corolarul 3.5. *Dacă E este o extindere algebrică a lui K şi F este o extindere algebrică a lui E, atunci F este o extindere algebrică a lui K.*

Demonstrație. Fie $\alpha \in F$. Cum α este algebric peste E există polinomul $f \in E[X]$, nenul, astfel încît $f(\alpha) = 0$.

Fie $f = b_0 + b_1X + \ldots + b_nX^n$ cu $b_0, b_1, \ldots, b_n \in E$. Dar, $f \in K(b_0, b_1, \ldots, b_n)$ $[X]$ și deci α este algebric peste $K(b_0, b_1, \ldots$ $\ldots, b_n)$. Rezultă că $K(b_0, b_1, \ldots, b_n)$ (α) este o extindere finită a lui $K(b_0, b_1, \ldots, b_n)$. Deoarece $b_0, b_1, \ldots, b_n$ sînt algebrice peste K, atunci $K(b_0, b_1, \ldots, b_n)$ este o extindere finită a lui K (vezi corolar 3.3). Rezultă din propoziția 1.2 că $K(b_0, b_1, \ldots, b_n, \alpha)$ este o extindere finită a lui K, deci algebrică. În particular, α este algebric peste K.

Corolarul 3.6. *Fie K un corp. Dacă*

$$\overline{K} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebric peste } K\},$$

atunci $\overline{K}$ este un subcorp al lui $\mathbb{C}$.

Demonstrație. Fie α, $\beta \in \overline{K}$. Avem $\alpha + \beta$, $\alpha\beta \in K(\alpha, \beta)$. Deoarece $K(\alpha, \beta)$ este o extindere finită a lui K, aceasta este algebrică și deci $\alpha + \beta$, $\alpha\,\beta \in \overline{K}$.

Analog, dacă $\alpha \in \overline{K}$ și $\alpha \neq 0$, atunci $\alpha^{-1} \in K(\alpha)$. Deoarece $K(\alpha)$ este o extindere finită a lui K, ea este și algebrică. Deci $\alpha^{-1} \in \overline{K}$. Corpul $\overline{K}$ se numește *închiderea algebrică* a lui K în $\mathbb{C}$. Deci $\mathbb{C} \setminus \overline{K}$ este mulțimea numerelor transcendente peste K.

Să luăm cazul particular cînd $K = \mathbb{Q}$. Corpul $\overline{\mathbb{Q}}$ se numește *mulțimea numerelor algebrice*.

§ 4. Extinderi simple

O extindere E a lui K se numește *simplă* dacă există un $\alpha \in E$ astfel încît $E = K(\alpha)$. Vom demonstra următoarea teoremă.

Teorema 4.1 (*a elementului primitiv*). *Dacă E este o extindere finită a lui K, atunci ea este simplă.*

Demonstrație. Fie $n = [E : K]$ și $\alpha_1, \alpha_2, \ldots, \alpha_n$ o bază a lui E peste K. Demonstrăm prin inducție după n. Dacă $n = 1$, atunci $E = K$. Presupunem $n = 2$. Atunci $E = K$ (α_1, α_2). Fie f_1 și f_2 polinoamele minimale ale numerelor α_1, respectiv α_2 peste corpul K.

Fie $\beta_1, \ldots, \beta_n$ ($\beta_1 = \alpha_1$) rădăcinile lui f_1 şi $\gamma_1, \ldots, \gamma_m$($\gamma_1 = \alpha_2$) rădăcinile lui f_2. Deoarece f_1 şi f_2 sînt ireductibile, atunci rădăcinile lui f_1 (respectiv ale lui f_2) sînt distincte.

Se consideră numerele

$$\frac{\beta_i - \beta_1}{\gamma_1 - \gamma_j}, \text{ unde } i = 1, \ldots, n \text{ şi } j = 2, \ldots, m. \qquad (2)$$

Numerele de forma (2) sînt în număr de $n(m - 1)$. Cum $\mathbb{Q}$ este infinit, există $c \in \mathbb{Q}$ care este diferit de toate numerele de forma (2). Punem $\theta = \alpha_1 + c\alpha_2 = \beta_1 + c\gamma_1$. Se vede uşor că $\theta \neq \beta_i + c\gamma_j$ ($1 \leqslant i \leqslant n$, $2 \leqslant j \leqslant m$). Numărul θ aparţine lui E şi deci $K(\theta) \subseteq E$.

Fie polinomul $g(X) = f_1(\theta - cX)$. Polinomul $g(X)$ aparţine lui $K(\theta)[X]$ şi $g(\alpha_2) = 0$. Cum şi $f_2 \in K(\theta)[X]$ şi $f_2(\alpha_2) = 0$, atunci α_2 este o rădăcină comună pentru g şi f_2. Dar $\theta \neq \beta_i + c\gamma_j$ ($1 \leqslant i \leqslant n$, $2 \leqslant j \leqslant m$) şi deci α_2 este singura rădăcină comună a lui f_2 şi g. Deci $X - \alpha_2$ este cel mai mare divizor comun a lui g şi f_2. Dar cum g şi f_2 sînt polinoame din $K(\theta)[X]$ atunci trebuie ca $X - \alpha_2$ să aparţină la $K(\theta)[X]$, adică α_2 aparţine la $K(\theta)$. Cum $\alpha_1 = \theta - c\alpha_2$, atunci α_1 este în $K(\theta)$ şi deci $E = K(\theta)$.

Această teoremă arată că mulţimea extinderilor finite, mulţimea extinderilor algebrice finit generate şi mulţimea extinderilor algebrice simple coincid.

§ 5. Extinderi normale

Fie K un corp; două numere α, β algebrice peste K se zic conjugate dacă au acelaşi polinom minimal.

Exemple. 1. Numerele $1 + i$ şi $1 - i$ sînt conjugate, deoarece sînt rădăcinile aceluiaşi polinom minimal $X^2 - 2X + 2 \in \mathbb{Q}[X]$.

2. Numerele $\sqrt{2} + \sqrt{3}$ şi $\sqrt{2} - \sqrt{3}$ sînt conjugate, deoarece sînt rădăcinile polinomului minimal $X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$.

O extindere E a lui K se numeşte *normală* peste K dacă E este o extindere finită a lui K şi orice număr conjugat cu un număr din E aparţine de asemenea lui E. Extinderile normale ale corpului $\mathbb{Q}$ se numesc *corpuri normale*.

Exemple. 1. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ este o extindere normală a lui $\mathbb{Q}$. Într-adevăr, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ şi conjugatul lui $a + b\sqrt{2}$ este $a - b\sqrt{2}$.

2. $\mathbb{C}$ este o extindere normală a lui $\mathbb{R}$.

Într-adevăr, $[\mathbb{C}:\mathbb{R}]=2$ şi conjugatul lui $a+bi$ este $a-ib$.

Pentru a da o formă echivalentă a noţiunii de extindere normală introducem noţiunea de corp de descompunere al unui polinom. Fie K un corp şi $f \in K[X]$ un polinom cu n=grad $(f) \geqslant \geqslant 1$. Din teorema lui d'Alembert f are n rădăcini complexe; fie acestea $\alpha_1, \alpha_2, \dots \alpha_n$. Corpul $K(\alpha_1, \alpha_2, \dots, \alpha_n)$ se numeşte *corpul de descompunere* peste K al lui f. Dacă $f \in \mathbb{Q}[X]$, atunci corpul de descompunere al lui f peste $\mathbb{Q}$ se numeşte, simplu, *corp de descompunere al lui f.*

Exemple. 1. Fie polinomul $f = X^4 - 2 \in \mathbb{Q}[X]$. Rădăcinile lui f sînt $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-i\sqrt[4]{2}$. Atunci, corpul de descompunere al lui f este $E = \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2})$.

2. Dacă se consideră acelaşi polinom $f = X^4 - 2$ dar cu coeficienţi în $\mathbb{R}[X]$, atunci corpul de descompunere al lui f peste $\mathbb{R}$ este $E = \mathbb{R}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbb{R}(i) = \mathbb{C}$.

Teorema 5.1. *Fie E o extindere a lui K. Atunci E este normală peste K dacă şi numai dacă E este corpul de descompunere al unui polinom cu coeficienţi din K.*

Demonstraţie. Presupunem mai întîi că E este normală peste K. Cum E este finită peste K, există $\alpha_1, \dots, \alpha_n \in E$ algebrice peste K astfel încît $E = K(\alpha_1, \dots, \alpha_n)$.

Fie f_i polinomul minimal al lui α_i peste K, oricare ar fi i, $1 \leqslant i \leqslant n$. Deoarece E este normală peste K, toate rădăcinile lui f_i aparţin lui E. Rezultă că toate rădăcinile polinomului $f = f_1 \dots f_n$ aparţin lui E. Dar $\alpha_1, \dots, \alpha_n$ se găsesc printre rădăcinile lui f şi deci E este corpul de descompunere al polinomului f peste K. Reciproc, presupunem că E este corpul de descompunere al polinomului $f \in K[X]$ şi $\alpha_1, \dots, \alpha_n$ rădăcinile lui f. Atunci $E = K(\alpha_1, \dots, \alpha_n)$ şi din corolarul 3.3 rezultă $K(\alpha_1, \dots, \alpha_n) = K[\alpha_1, \dots, \alpha_n]$. Dacă $\beta \in E$, atunci există un polinom $g \in K[X_1, \dots, X_n]$ astfel încît $\beta = g(\alpha_1, \dots, \alpha_n)$. Fie σ_n grupul permutărilor de n elemente; atunci, pentru fiecare $\sigma \in \sigma_n$ notăm cu $g_\sigma(X_1, \dots, X_n)$ polinomul $g(X_{\sigma(1)}, \dots, X_{\sigma(n)})$. Fie polinomul $G(X_1, \dots, X_n, X) \in K[X_1, \dots, X_n][X]$ definit prin egalitatea

$$G(X_1, \dots, X_n, X) = \prod_{\sigma \in \sigma_n} (X - g_\sigma(X_1, \dots, X_n)) \qquad (3)$$

al cărui grad este $n\,!$. Scriem toate permutările lui σ_n în ordinea

$$\sigma_1 = e, \ \sigma_2, \dots, \sigma_{n\,!},$$

unde e este permutarea identică. De asemenea, polinomul $G(X_1, \ldots, X_n, X)$ se scrie sub forma

$$G(X_1, \ldots, X_n, X) = X^{n!} - A_1 X^{n!-1} + A_2 X^{n!-2} + \ldots + (-1)^{n!} A_{n!},$$

unde

$$A_1 = g_{\sigma_1} + g_{\sigma_2} + \ldots + g_{\sigma_{n!}},$$

$$A_2 = g_{\sigma_1} \cdot g_{\sigma_2} + g_{\sigma_1} \cdot g_{\sigma_3} + \ldots + g_{\sigma_{n!-1}} \cdot g_{\sigma_{n!}},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$A_{n!} = g_{\sigma_1} g_{\sigma_2} \ldots g_{\sigma_{n!}}.$$

Dacă σ este o permutare arbitrară, atunci elementele $\sigma \cdot \sigma_1$, $\sigma \cdot \sigma_2, \ldots, \sigma \cdot \sigma_{n!}$ sînt diferite între ele şi în număr de $n!$. Deci $\{\sigma \cdot \sigma_1, \sigma \cdot \sigma_2, \ldots, \sigma \cdot \sigma_{n!}\}$ este egală cu sistemul $\{\sigma_1, \sigma_2, \ldots$ $\ldots, \sigma_{n!}\}$, eventual într-o altă ordine. Rezultă că polinoamele $A_1, A_2, \ldots, A_{n!}$ sînt polinoame simetrice în variabilele $X_1, \ldots$ $\ldots, X_n$. Făcînd în (1) $X_1 = \alpha_1, X_2 = \alpha_2, \ldots, X_n = \alpha_n$, se obţine polinomul

$$\bar{G}(X) = G(\alpha_1, \alpha_2, \ldots, \alpha_n, X).$$

Dacă notăm $\beta_i = g_{\sigma_i}(\alpha_1, \ldots, \alpha_n)$, unde $i = 1, 2, \ldots, n!$, atunci

$$\bar{G}(X) = \prod_{i=1}^{n!} (X - \beta_i).$$

Coeficienţii lui $\bar{G}(X)$ sînt elementele $a_i = A_i(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Deoarece $A_i(X_1, \ldots, X_n)$ sînt polinoame simetrice de $X_1, \ldots$ $\ldots, X_n$, rezultă $a_i \in K$ pentru orice $i = 1, 2, \ldots, n!$. Deci $\bar{G}(X)$ este un polinom din $K[X]$. Întrucît $\beta = \beta_1 = g(\alpha_1, \alpha_2, \ldots$ $\ldots, \alpha_n)$, rezultă că β este rădăcină a lui $\bar{G}(X)$. Fie $h(X)$ polinomul minimal al lui β peste K. Din $\bar{G}(\beta) = 0$ rezultă că h divide pe $\bar{G}$, deci, rădăcinile lui h se găsesc printre rădăcinile lui $\bar{G}$ care sînt în E. Aşadar, E este o extindere normală a lui K.

§ 6. Automorfismele unei extinderi

Fie K şi K' două corpuri. Amintim că o aplicaţie $\sigma : K \to K'$ şi se numeşte *omomorfism* (*de corpuri*) dacă are proprietăţile:

1° pentru orice $x, y \in K$ avem $\sigma(x + y) = \sigma(x) + \sigma(y)$, $\sigma(xy) = \sigma(x) \cdot \sigma(y)$;
2° $\sigma(1) = 1$.

Observații. 1. Dacă $x \in X$, $x \neq 0$, atunci $\sigma(x^{-1}) = \sigma(x)^{-1}$. Într-adevăr, $1 = \sigma(1) = \sigma(xx^{-1}) = \sigma(x) \cdot \sigma(x^{-1})$, de unde rezultă $\sigma(x^{-1}) = \sigma(x)^{-1}$.

2. σ este injectivă. Într-adevăr, trebuie să arătăm că din $\sigma(x) = 0$ rezultă $x = 0$. Dacă $x \neq 0$, atunci $1 = \sigma(xx^{-1}) = \sigma(x) \cdot \sigma(x^{-1}) = 0$, ceea ce constituie o contradicție.

Un omomorfism de corpuri $\sigma : K \to K'$ care este bijectiv se numește *izomorfism (de corpuri)*. Deci, ca $\sigma : K \to K'$ să fie izomorfism este suficient să fie surjectiv.

Dacă $\sigma : K \to K$ este un izomorfism de corpuri, σ se numește *automorfism*.

Propoziția 6.1. 1) *Compunerea a două omomorfisme de corpuri este omomorfism de corpuri.*

2) *Dacă $\sigma : K \to K'$ este un izomorfism de corpuri, atunci funcția inversă $\sigma^{-1} : K' \to K$ este un izomorfism de corpuri.*

Demonstrație. Afirmația 1) este imediată. Să verificăm 2). Fie x', $y' \in K'$; cum σ este surjectivă, există $x, y \in K$ astfel încît $\sigma(x) = x'$ și $\sigma(y) = y'$. Atunci

$$\sigma^{-1}(x' + y') = \sigma^{-1}(\sigma(x) + \sigma(y)) = \sigma^{-1}(\sigma(x + y)) = x + y.$$

Dar

$$\sigma^{-1}(x') = \sigma^{-1}(\sigma(x)) = x \text{ și } \sigma^{-1}(y') = \sigma^{-1}(\sigma(y)) = y,$$

de unde obținem $\sigma^{-1}(x' + y') = \sigma^{-1}(x') + \sigma^{-1}(y')$. Analog, rezultă $\sigma^{-1}(x'y') = \sigma^{-1}(x') \cdot \sigma^{-1}(y')$.

Deoarece $\sigma(\sigma^{-1}(1)) = 1 = \sigma(1)$ și ținînd seama că σ este injectivă, obținem $\sigma^{-1}(1) = 1$. Deci σ^{-1} este un omomorfism de corpuri. Cum σ este bijectivă, și σ^{-1} este bijectivă.

Fie E și F două extinderi ale corpului K. Un omomorfism (respectiv izomorfism) de corpuri $\sigma : E \to F$ cu proprietatea $\sigma(x) = x$, oricare ar fi $x \in K$, se numește *K-omomorfism* (respectiv *K-izomorfism*). Dacă E este o extindere a lui K și $\sigma : E \to E$ este un K-izomorfism, σ se numește *K-automorfism*.

Propoziția 6.2. *Dacă E este o extindere algebrică a lui K și $\sigma : E \to E$ un K-omomorfism, atunci σ este un K-automorfism.*

Demonstrație. Fie $\alpha \in E$ care este algebric peste K. Fie f polinomul minimal al lui α. Notăm

$$X_\alpha = \{\beta \in E \mid f(\beta) = 0\}.$$

Este clar că $\alpha \in X_\alpha$ şi X_α este o mulţime finită. Dacă $\beta \in X_\alpha$, atunci $\sigma(\beta)$ este de asemenea o rădăcină a polinomului. Într-adevăr, scriem

$$f = a_0 + a_1X + \dots + a_n X^n,$$

$$a_0, a_1, \dots, a_n \in K.$$

$f(\beta) = 0$ implică $a_0 + a_1\beta + \dots + a_n \beta^n = 0$. Aplicînd pe σ, obţinem

$0 = \sigma(0) = \sigma(a_0 + a_1\beta + \dots + a_n\beta^n) = \sigma(a_0) + \sigma(a_1)\sigma(\beta) + \dots + \sigma(a_n)\sigma(\beta)^n = a_0 + a_1 \sigma(\beta) + \dots + a_n\sigma(\beta)^n$, de unde rezultă că $f(\sigma(\beta)) = 0$, adică $\sigma(\beta) \in X_\alpha$. Rezultă deci că $\sigma(X_\alpha) \subseteq X_\alpha$. Cum X_α este finită şi σ este o funcţie injectivă, atunci $\sigma(X_\alpha) = X_\alpha$. Dar $E = \bigcup_{\alpha \in E} X_\alpha$ şi deci

$$\sigma(E) = \sigma(\bigcup_{\alpha \in E} X_\alpha) = \bigcup_{\alpha \in E} \sigma(X_\alpha) = \bigcup_{\alpha \in E} X_\alpha = E.$$

Rezultă că σ este surjectivă şi deci bijectivă.

§ 7. Grupul Galois asociat unei extinderi normale

Fie E o extindere arbitrară a lui K. Se notează $G(E/K)$ mulţimea K-automorfismelor lui E. Din propoziţia 6.1 rezultă că $G(E/K)$ împreună cu operaţia de compunere a funcţiilor este un grup. Elementul neutru al acestui grup este funcţia identică

$$1_E : E \to E, \qquad 1_E(x) = x.$$

Grupul $G(E/K)$ se numeşte *grupul lui Galois* asociat extinderii E.

Ne vom ocupa, în mod deosebit, de studiul grupului lui Galois asociat unei extinderi normale.

Propoziţia 7.1. *Fie E o extindere normală a lui K. Atunci $G(E/K)$ este un grup finit avînd ordinul egal cu $[E : K]$.*

Demonstrație. Cum E este o extindere finită, atunci, din teorema 4.1 rezultă că există $\theta \in E$ astfel încît $E = K(\theta)$. Fie $f = a_0 + a_1X + \ldots + a_nX^n$ polinomul minimal al lui θ. Din propoziția 3.2 rezultă că $n = [E : K]$ și orice element $\alpha \in E$ se scrie în mod unic sub forma $\alpha = c_0 + c_1\theta + \ldots + c_{n-1}\theta^{n-1}$, unde $c_0, c_1, \ldots, c_{n-1} \in K$.

Să notăm cu X mulțimea rădăcinilor polinomului f. Este clar că θ aparține lui X, care are n elemente și $X \subseteq E$, deoarece E este o extindere normală a lui K. Dacă $x \in X$, atunci $\sigma(x) \in X$, pentru orice $\sigma \in G(E/K)$.

Definim aplicația

$$\varphi : G(E/K) \to X$$

prin $\varphi(\sigma) = \sigma(\theta)$, unde $\sigma \in (E/K)$. Dacă arătăm că φ este bijectivă, totul este demonstrat. Fie că $\varphi(\sigma) = \varphi(\sigma')$, adică $\sigma(\theta) = \sigma'(\theta)$. Atunci

$$\sigma(\alpha) = \sigma(c_0 + c_1\theta + \ldots + c_{n-1}\theta^{n-1}) = \sigma(c_0) + \sigma(c_1)\,\sigma(\theta) + \ldots$$

$$\ldots + \sigma(c_{n-1})\,\sigma(\theta^{n-1}) = c_0 + c_1\,\sigma(\theta) + \ldots + c_{n-1}\,\sigma(\theta)^{n-1}.$$

Analog, $\sigma'(\alpha) = c_0 + c_1\,\sigma'(\theta) + \ldots + c_{n-1}\,\sigma'(\theta)^{n-1}$ și deci $\sigma(\alpha) = \sigma'(\alpha)$. Cum α este arbitrar, rezultă că $\sigma = \sigma'$ și deci φ este injectivă.

Fie θ' un element din X și definim $\sigma : E \to E$ în felul următor. Dacă α este un element oarecare al lui E și cum $E = K(\theta) = K[\theta]$, atunci există $g \in K[X]$ astfel încît $\alpha = g(\theta)$. Punem prin definiție $\sigma(\alpha) = g(\theta')$. Dacă $\alpha = g(\theta) = g_1(\theta)$, unde g, $g_1 \in K[X]$, atunci $(g - g_1)(\theta) = 0$ și deci f divide pe $g - g_1$, adică $g - g_1 = f \cdot f_1$. Cum θ' este rădăcină a lui f, avem $g(\theta') = g_1(\theta') = f(\theta')f_1(\theta') = 0$. Deci $g(\theta') = g_1(\theta')$, ceea ce înseamnă că σ este bine definită. Dacă $\beta \in E$ este un alt element, există un $h \in K[X]$ astfel încît $\beta = h(\theta)$. Atunci $\alpha + \beta = g(\theta) + h(\theta) = (g + h)(\theta)$ și deci

$$\sigma(\alpha + \beta) = (g + h)(\theta') = g(\theta') + h(\theta') = \sigma(\alpha) + \sigma(\beta).$$

Analog, avem $\sigma(\alpha\beta) = \sigma(\alpha) \cdot \sigma(\beta)$.

Dacă $\alpha \in K$, atunci după definiția lui σ avem $\sigma(\alpha) = \alpha$ și deci σ este K-omomorfism. Din propoziția 6.2 rezultă că σ este un K-automorfism și deci $\sigma \in G(E/K)$. Cum $\sigma(\theta) = \theta'$, atunci $\varphi(\sigma) = \theta'$ și deci φ este surjectivă.

Observație. Din demonstrație rezultă că dacă E este o extindere finită a lui K (nu neapărat normală), atunci $G(E/K)$ este un grup finit avînd ordinul $\leqslant [E:K]$.

Exemplu. Fie $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$. Este clar că $[(\mathbb{Q}\sqrt{3}) : \mathbb{Q}] = 2$ și $\mathbb{Q}(\sqrt{3})$ este o extindere normală a lui $\mathbb{Q}$, ca fiind corpul de descompunere al polinomului $X^2 - 3$. Rezultă că grupul Galois $G(\mathbb{Q}\sqrt{3})/\mathbb{Q})$ are două elemente și anume aplicația identică a lui $\mathbb{Q}(\sqrt{3})$ și automorfismul

$$\sigma : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{3}),\ \sigma(a + b\sqrt{3}) = a - b\sqrt{3}.$$

§ 8. Compozitul a două corpuri

Fie K_1 și K_2 două corpuri. Se numește *compozitul* celor două corpuri cel mai mic corp K care conține atît pe K_1 cît și pe K_2. Existența lui K rezultă din faptul că acesta este egal cu intersecția tuturor corpurilor ce conțin în același timp ambele corpuri K_1 și K_2. Corpul K se notează K_1K_2 și este dat de formula

$$K_1K_2 = \left\{ \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{j=1}^{n} z_j t_j} \;\middle|\; x_1,\ldots,x_m;\ z_1,\ldots,z_n \in K_1;\ y_1,\ldots,y_m;\ t_1,\ldots,t_n \in K_2 \right\}.$$

Pentru a verifica aceasta, să notăm cu K partea a doua a egalității; se vede ușor că K este un corp ce conține pe K_1 și K_2 și deci $K_1K_2 \subseteq K$. Fie acum E un alt corp ce conține pe K_1 și K_2. Atunci orice element de forma

$$\frac{\sum_{i=1}^{m} x_i y_i}{\sum_{j=1}^{n} z_j t_j} \quad x_1, \ldots, x_m, z_1, \ldots, z_n \in K_1;\ y_1, \ldots, y_m, t_1, \ldots, t_n \in K_2,$$

aparține lui E și deci $K \subseteq E$. Prin urmare, avem și $K \subseteq K_1K_2$, adică egalitatea $K_1K_2 = K$.

Dacă K este un corp, $E = K(\alpha_1, \ldots, \alpha_m)$ și $F = K(\beta_1, \ldots, \beta_n)$, atunci $EF = K(\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \ldots, \beta_n)$.

Propoziția 8.1. *Dacă E și F sînt două extinderi finite ale unui corp K, atunci EF este o extindere finită a lui K. Mai*

mult, dacă E şi F sînt extinderi normale ale lui K, atunci EF este o extindere normală a lui K.

Demonstraţie. Putem scrie că $E = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$ şi $F = K(\beta_1, \ldots, \beta_n) \Rightarrow$ unde $(\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ sînt algebrice peste K. Cum $EF = K(\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$, atunci după corolarul 3.3 rezultă că EF este o extindere finită a lui K.

Fie E şi F extinderi normale ale lui K. Atunci E este corpul de descompunere al unui polinom $f \in K[X]$, iar F este corpul de descompunere al unui polinom $g \in K[X]$. Dacă $\alpha_1, \ldots, \alpha_m$ sînt rădăcinile lui f şi $\beta_1, \ldots, \beta_n$ ale lui g, atunci $E = K(\alpha_1, \ldots, \alpha_m)$ şi $F = K(\beta_1, \ldots, \beta_n)$. Cum $EF = K(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$ şi $\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ sînt rădăcinile polinomului fg, rezultă că EF este corpul de descompunere al polinomului fg. Deci EF este o extindere normală peste K.

Propoziţia 8.2. *Fie E şi F două extinderi ale lui K astfel încît E este normală peste K. Atunci EF este o extindere normală a lui F.*

Demonstraţie. E fiind normală peste K, există polinomul $f \in K[X]$ astfel încît E este corpul de descompunere al lui f. Dacă $\alpha_1, \ldots, \alpha_n$ sînt rădăcinile lui f, atunci $E = K(\alpha_1, \ldots, \alpha_n)$. Dar $EF = F(\alpha_1, \ldots, \alpha_n)$ şi cum $f \in F[X]$, rezultă că EF este corpul de descompunere al lui f peste corpul F. Deci EF este o extindere normală a lui F.

Mai sus s-a definit compozitul a două corpuri. Se poate defini compozitul unui număr finit de corpuri $K_1, K_2, \ldots, K_n$ ca fiind cel mai mic corp K care le conţine pe toate. Acest corp există şi este egal cu intersecţia tuturor corpurilor ce conţin pe $K_1, K_2, \ldots, K_n$; se va nota prin $K_1K_2 \ldots K_n$. Se vede uşor că $K_1K_2 \ldots K_n$ este compozitul corpurilor $K_1K_2 \ldots K_i$ şi $K_{i+1} \ldots K_n$, unde $1 \leqslant i \leqslant n$.

§ 9. Corespondenţa lui Galois

Fie E o extindere normală a corpului K. Se va nota cu G grupul Galois $G(E/K)$. De asemenea, se notează cu $\mathcal{E}_{E/K}$ mulţimea extinderilor lui K conţinute în E iar cu $\mathcal{L}(G)$ mulţimea subgrupurilor lui G. Fie $F \in \mathcal{E}_{E/K}$. Cum E este o extindere normală a lui K, atunci E este o extindere normală şi a lui F.

Observăm că $G(E/F)$ este un subgrup al lui G. Definim atunci aplicația

$$\varphi : \mathscr{E}_{E/K} \to \mathscr{L}(G)$$

prin $\varphi(F) = G(E/F)$.

Fie H un subgrup al lui G. Notăm

$$E^H = \{x \in E \mid \sigma(x) = x, \text{ oricare } \sigma \in H\}.$$

Se vede ușor că E^H este un corp și $K \subseteq E^H \subseteq E$.

Fie, de asemenea, aplicația

$$\psi : \mathscr{L}(G) \to \mathscr{E}_{E/K}, \ \psi(H) = E^H.$$

Lema 9.1. *Cu notațiile de mai sus, are loc egalitatea* $G(E/E^H) = H$.

Demonstrație. Incluziunea $H \subseteq G(E/E^H)$ este evidentă. Există $\theta \in E$ astfel încît $E = E^H(\theta)$. Fie $\sigma_1, \ldots, \sigma_r \in H$ în număr maxim, astfel încît mulțimea $\{\sigma_1(\theta), \ldots, \sigma_r(\theta)\}$ este formată din elemente distincte. Putem presupune că $\sigma_1 = 1_E$.

Fie polinomul

$$f = \prod_{i=1}^{r} (X - \sigma_i(\theta)).$$

Dacă $\sigma \in H$ este arbitrar, atunci sistemul de elemente $\{\sigma\sigma_1(\theta), \ldots, \sigma\sigma_r(\theta)\}$ este același cu sistemul de elemente $\{\sigma_1(\theta), \ldots, \sigma_r(\theta)\}$, eventual în altă ordine. Scriind pe f sub forma

$$f = X^r - a_1X^{r-1} + a_2X^{r-2} + \ldots + (-1)^r a_r,$$

avem

$$a_1 = \sigma_1(\theta) + \ldots + \sigma_r(\theta),$$

$$a_2 = \sigma_1(\theta)\,\sigma_2(\theta) + \sigma_1(\theta)\,\sigma_3(\theta) + \ldots + \sigma_{r-1}(\theta)\sigma_r(\theta),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_r = \sigma_1(\theta) \ldots \sigma_r(\theta).$$

Rezultă că $\sigma(a_i) = a_i$ pentru orice $\sigma \in H$ și deci $a_i \in E^H$ $(1 \leqslant i \leqslant r)$. Deci f este un polinom cu coeficienți în E^H, θ fiind rădăcină a sa. Dacă g este polinomul minimal al lui θ peste corpul

E^H, atunci g divide pe f. După propoziția 7.1 avem ord $G(E/E^H) = [E : E^H] = \text{grad } g \leqslant \text{grad } f = r$. Deci ord $G(E/E^H) \leqslant$ ord H, de unde rezultă imediat egalitatea $H = G(E/E^H)$.

Lema 9.2. *Dacă F este un corp cuprins între K și E și $H = G(E/F)$, atunci $E^H = F$.*

Demonstrație. După propoziția 7.1 avem ord $H = [E : F]$ iar după lema 9.1 avem $[E : E^H] =$ ord H. Deci $[E : F] = [E : E^H]$. Este evident că $F \subseteq E^H$, de unde avem $[E : F] = [E : E^H] \cdot [E^H : F]$; rezultă că $[E^H : F] = 1$ și deci $E^H = F$.

Lema 9.3. *Fie F un corp cuprins între K și E. Atunci F este o extindere normală a lui K dacă și numai dacă subgrupul $H = G(E/F)$ este un subgrup normal al lui G. Mai mult, $G(F/K) \simeq G/H$.*

Demonstrație. Presupunem mai întîi că F este normală peste K și notăm cu $G' = G(F/K)$. Cum F este normală, există un polinom $f \in K[X]$ astfel încît $F = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, unde $\alpha_1, \alpha_2, \ldots, \alpha_n$ sînt rădăcinile lui f. Fie acum $u \in G$. Întrucît u este K-omomorfism, atunci $u(\alpha_1), \ldots, u(\alpha_n)$ sînt rădăcini ale lui f. Dar $F = K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \alpha_2, \ldots, \alpha_n]$ și deci $u(F) = u(K[\alpha_1, \ldots, \alpha_n]) = K[u(\alpha_1), \ldots, u(\alpha_n)] \subseteq K[\alpha_1, \alpha_2, \ldots, \alpha_n] = F$. Așadar, $u(F) \subseteq F$ și după propoziția 6.2 rezultă că $u(F) = F$. Are sens să definim aplicația

$$\varphi : G \to G', \quad \varphi(u) = u|F.$$

Se arată ușor că φ este omomorfism de grupuri al cărui nucleu este

Ker $\varphi = \{u \in G \mid \varphi(u) = 1_F\} = \{u \in G \mid u|F = 1_F\} = \{u \in G \mid u(\alpha) = \alpha$, oricare ar fi $\alpha \in F\} = H$. Cum Ker φ este un subgrup normal, atunci H este subgrup normal. După teorema fundamentală de izomorfism de la grupuri avem Im $\varphi \simeq G/\text{Ker } \varphi = G/H$ iar din teorema lui Lagrange

$$\text{ord Im } \varphi = \frac{\text{ord } G}{\text{ord} H}.$$

Deoarece ord $G = [E : K]$, ord $H = [E : F]$ și ord $G' = [F : K]$, avem

$$\text{ord Im } \varphi = \frac{[E : K]}{[E : F]} = \frac{[E : F] \cdot [F : K]}{[E : F]} = [F : K].$$

Deci ord Im φ = ord G' şi deoarece Im φ este un subgrup al lui G', rezultă Im $\varphi = G'$. Aşadar $G' \simeq G/H$.

Teorema fundamentală a teoriei Galois. *Fie E o extindere normală a lui K şi $G = G(E/K)$ grupul Galois asociat. Notăm cu $\mathcal{E}_{E/K}$ mulţimea subcorpurilor F cuprinse între K şi E iar cu $\mathcal{L}(G)$ mulţimea subgrupurilor H ale lui G.*

Considerăm aplicaţiile

$$\varphi : \mathcal{E}_{E/K} \to \mathcal{L}(G), \ \varphi(F) = G(E/F),$$

$$\psi : \mathcal{L}(G) \to \mathcal{E}_{E/K}, \ \psi(H) = E^H.$$

Atunci:

1) $\psi \circ \varphi = 1_{\mathcal{E}_{E/K}}$ *şi* $\varphi \circ \psi = 1_{\mathcal{L}(G)}$;

2) *F este normală peste K dacă şi numai dacă $H = G(E/F)$ este un subgrup normal al lui G. În acest caz, dacă notăm $G' = G(F/K)$, atunci $G' \simeq G/H$;*

3) *ord $G(E/F) = [E : F]$ pentru orice $F \in \mathcal{E}_{E/K}$ şi ord $H = [E : E^H]$ pentru orice $H \in \mathcal{L}(G)$.*

Demonstraţia acestei teoreme este o consecinţă imediată a celor trei leme de mai înainte.

Vom indica, drept aplicaţie a teoremei fundamentale a lui Galois, următoarea teoremă:

Teorema elementelor conjugate. *Fie E o extindere normală a corpului K şi α, β două elemente din E care sînt conjugate. Atunci există $u \in G(E/K)$ astfel încît $u(\alpha) = \beta$.*

Demonstraţie. Fie $\sigma_1, \sigma_2, \ldots, \sigma_r$ elemente din $G = G(E/K)$ în număr maxim, astfel încît $\sigma_1(\alpha), \ldots, \sigma_r(\alpha)$ sînt distincte. Putem presupune că $\sigma_1 = 1_E$. Considerăm polinomul

$$g = \prod_{i=1}^{r} (X - \sigma_i(\alpha)).$$

După demonstraţia lemei 9.1 rezultă că g este un polinom cu coeficienţi în E^G. Dar, după teorema fundamentală a lui Galois, $E^G = K$ şi deci $g \in K[X]$. Fie $f \in K[X]$ polinomul minimal al lui α. Deoarece $g(\alpha) = 0$, atunci f divide pe g şi deci rădăcinile lui f se găsesc printre rădăcinile lui g. Dar β, fiind o rădăcină a lui f, va fi rădăcină a lui g. Există atunci un i, $1 \leqslant i \leqslant k$, astfel încît $\beta = \sigma_i(\alpha)$.

§ 10. Calculul grupului lui Galois

Propoziția 10.1. *Fie E o extindere normală a corpului K, G grupul Galois al său și F o extindere arbitrară a lui K astfel încît $E \cap F = K$. Atunci EF este o extindere normală a lui F și dacă $H = G(EF/F)$, atunci $H \simeq G$.*

Demonstrație. Faptul că EF este o extindere normală a lui F rezultă din propoziția 8.2. Definim $\varphi : H \to G$, $\varphi(u) = u|E$ [această aplicație are sens deoarece din faptul că E este normală rezultă $u(E) = E$]. Este clar că φ este omomorfism de grupuri. Să dovedim că φ este un izomorfism. Dacă $u \in \text{Ker } \varphi$, atunci $u|E = 1_E$, adică $u(x) = x$, oricare ar fi $x \in E$.

Fie $z \in EF$ un element arbitrar. Atunci

$z = \dfrac{\sum_{i=1}^{m} x_i y_i}{\sum_{j=1}^{n} x'_j y'_j}$, unde toți x_i, $x'_j \in E$ și y_i, $y'_j \in F$. Dar din faptul că $u \in H$ rezultă că u este F-omomorfism. Deci

$$u(z) = \frac{\sum_{i=1}^{m} u(x_i)\, u(y_i)}{\sum_{j=1}^{n} u(x'_j)\, u(y'_j)} = \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{j=1}^{n} x'_j y'_j} = z.$$

Deci $u(z) = z$, oricare ar fi $z \in EF$, adică $u = 1_{EF}$. Prin urmare, Ker $\varphi = \{1_{EF}\}$ și deci φ este injectivă. Să demonstrăm că φ este și surjectivă. Fie $G' = \text{Im } \varphi$. Din teorema fundamentală a teoriei lui Galois avem $G' = G$ dacă și numai dacă $E^{G'} = E^G = K$. Deci, trebuie verificat că $E^{G'} = K$. Dacă $\alpha \in E^{G'}$, atunci $v(\alpha) = \alpha$, oricare ar fi $v \in G'$. Dar există $u \in H$ astfel încît $\varphi(u) = v$ și deci $v = u|E$. Așadar, $u(\alpha) = \alpha$, oricare ar fi $u \in H$ sau $\alpha \in EF^H = F$ (din teorema fundamentală a lui Galois). Cum $\alpha \in E$, atunci $\alpha \in E \cap F = K$ și deci $E^{G'} = K$. Prin urmare, $G' = G$, deci φ este și surjectivă.

Teorema 10.2. *Fie E_1 și E_2 două extinderi normale ale lui K cu grupurile Galois G_1 și G_2 asociate. Atunci E_1E_2 este o extindere normală a lui K și dacă $E_1 \cap E_2 = K$, atunci $G(E_1E_2/K) \simeq G_1 \times G_2$.*

Demonstrație. Faptul că E_1E_2 este o extindere normală a lui K rezultă din propoziția 8.1. Să notăm $G = G(E_1E_2/K)$. Definim aplicația $\varphi : G \to G_1 \times G_2$ prin $\varphi(u) = (u|E_1, u|E_2)$. Este evident că φ este omomorfism de grupuri. Să dovedim că φ este un izomorfism. Mai întîi, să arătăm că φ este injectivă. Fie $u \in \in \operatorname{Ker} \varphi$. Atunci $(u|E_1, u|E_2) = (1_{E_1}, 1_{E_2})$, adică $u(x) = x$, oricare ar fi $x \in E_1$, și $u(y) = y$, pentru orice $y \in E_2$.

Fie $z \in E_1E_2$; atunci $z = \dfrac{\sum_{i=1}^{m} x_i y_i}{\sum_{j=1}^{n} x'_j y'_j}$, unde toți x_i, $x'_j \in E_1$ și toți y_i, $y'_j \in E_2$. Deci

$$u(z) = \frac{\sum_{i=1}^{m} u(x_i)\, u(y_i)}{\sum_{j=1}^{n} u(x'_j) u(y'_j)} = \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{j=1}^{n} x'_j y'_j} = z.$$

Așadar, $u = 1_{E_1E_2}$ și deci φ este injectivă.

Să arătăm că φ este surjectivă. Fie $(v_1, v_2) = G_1 \times G_2$. Din propoziția 10.1 pentru v_1 există $u_1 : E_1E_2 \to E_1E_2$ care este un E_2-omomorfism astfel încît $u_1|E_1 = v_1$. Atunci $\varphi(u_1) = (u_1|E_1, u_1|E_2) = (v_1, 1_{E_2})$. Analog, pentru v_2 există $u_2 : E_1E_2 \to E_1E_2$ care este un E_1-omomorfism astfel încît $u_2|E_2 = v_2$. Atunci $\varphi(u_2) = (1_{E_2}, v_2)$. Dacă punem $u = u_1u_2$, atunci $\varphi(u) = \varphi(u_1u_2) = \varphi(u_1)\, \varphi(u_2) = (v_1, 1_{E_2}) \cdot (1_{E_1}, v_2) = (v_1, v_2)$ și deci φ este surjectivă.

Corolarul 10.3. *Fie K un corp și $E_1, E_2, \ldots, E_n$ extinderi normale ale lui K astfel încît $E_i \cap (E_{i-1} E_{i+1} \ldots E_n) = K$, pentru orice $i = 1, 2, \ldots, n$. Dacă G_i este grupul lui Galois al extinderii E_i peste K $(1 \leqslant i \leqslant n)$ și G grupul lui Galois al extinderii $E_1E_2 \ldots E_n$, atunci $G \simeq G_1 \times G_2 \times \ldots \times G_n$.*

Demonstrație. Demonstrăm prin inducție după n. Pentru $n = 2$ demonstrația rezultă din teorema precedentă. Deoarece $E_n \cap (E_1 \ldots E_{n-1}) = K$, din aceeași teoremă avem $G \simeq \simeq G(E_1 \ldots E_{n-1}/K) \times G_n$. Din ipoteza de inducție rezultă că $G(E_1 \ldots E_{n-1}/K) \simeq G_1 \times G_2 \times \ldots \times G_{n-1}$, de unde se obține $G \simeq G_1 \times \ldots \times G_n$.

Exemplu. Fie $p_1, p_2, \ldots, p_n$ numere prime distincte. Considerăm corpul $E = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$. Dacă $E_i = \mathbb{Q}(\sqrt{p_i})$, atunci $E = E_1 E_2 \ldots E_n$. Se

vede ușor că $E_i \cap (E_1 \ldots E_{i-1}E_{i+1} \ldots E_n)=\mathbb{Q}$, oricare ar fi i, $i=1, 2, \ldots, n$. Să notăm $G_i = G(E_i/\mathbb{Q}) \cdot G_i$ are două elemente, deci $G_i \simeq \mathbb{Z}_2$. Aplicînd corolarul precedent, rezultă

$$G(E/\mathbb{Q}) \simeq G_1 \times G_2 \times \ldots \times G_n \simeq \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{n \text{ factori}}.$$

§ 11. Grupul Galois al unui polinom

Fie K un corp și f un polinom din $K[X]$ de grad $(f) \geqslant 1$.

Să notăm cu E corpul de descompunere al lui f, care este o extindere normală a lui K. Grupul $G = G(E/K)$ se numește *grupul Galois asociat polinomului f.*

Propoziția 11.1. *Fie $f \in K[X]$ un polinom ireductibil cu $n =$ grad $(f) \geqslant 1$. Dacă G este grupul Galois al acestui polinom, atunci G este izomorf cu un subgrup al lui σ_n.*

Demonstrație. Dacă $X = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ sînt rădăcinile lui f, atunci $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Fie $u \in G$. Cum u este un K-omomorfism, atunci $u(\alpha_i)$ este o rădăcină a lui f. Deci $u(X) \subseteq$ $\subseteq X$ și cum u este injectivă, rezultă $u(X) = X$. Dar f este ireductibil, deci $\alpha_1, \alpha_2, \ldots, \alpha_n$ sînt distincte între ele. Să notăm cu S_X mulțimea aplicațiilor bijective ale lui X în X. Deci S_X este un grup care este izomorf cu σ_n.

Definim $\varphi : G \to S_X$, $\varphi(u) = u|X$. Este evident că φ este un omomorfism de grupuri. Să dovedim că φ este injectivă, adică, să verificăm că Ker $\varphi = \{1_E\}$. Dacă $u \in$ Ker φ, atunci $u|X = 1_X$, adică $u(\alpha_i) = \alpha_i$ $(1 \leqslant i \leqslant n)$. Deoarece $E=K(\alpha_1, \alpha_2, \ldots, \alpha_n) =$ $= K[\alpha_1, \alpha_2, \ldots, \alpha_n]$, fie $x \in K[\alpha_1, \ldots, \alpha_n]$. Există $f \in K[X_1, \ldots$ $\ldots, X_n]$ astfel încît $x = f(\alpha_1, \ldots, \alpha_n)$. Dar atunci $u(x) =$ $=u(f(\alpha_1, \ldots, \alpha_n)) = f(u(\alpha_1), \ldots, u(\alpha_n)) = f(\alpha_1, \ldots, \alpha_n)=x$. Deci $u = 1_E$. Cum φ este injectivă, rezultă că $G \simeq$ Im φ. Dar Im φ este un subgrup în S_X și deci este izomorf cu un subgrup al lui σ_n. Deci G este izomorf cu un subgrup al lui σ_n.

Fie G un subgrup al lui σ_n. Subgrupul G se numește *tranzitiv* dacă, oricare ar fi $1 \leqslant i, j \leqslant n$, există o permutare $\sigma \in G$ astfel încît $\sigma(i) = j$.

Propoziția 11.2. *Fie G un subgrup al lui σ_n. Presupunem că : 1° n este număr prim ; 2° G este tranzitiv ; 3° G conține o transpoziție. Atunci $G = \sigma_n$.*

Demonstrație. Fie (i_1, i_2) o transpoziție ce aparține lui G. Fie m numărul maxim astfel încît $(i_1, i_2), \ldots, (i_1, i_m) \in G$. Este evident că $m \leqslant n$. Fie $1 \leqslant p$, $q \leqslant m$. Atunci, deoarece $(i_p, i_q) = (i_1, i_p)(i_1, i_q)(i_1, i_q)$, rezultă că $(i_p, i_q) \in G$.

Fie j un număr natural astfel încît $1 \leqslant j \leqslant n$ și $j \notin \{i_1, \ldots, i_m\}$. Atunci $(j, i_p) \notin G$, pentru orice $1 \leqslant p \leqslant m$. Într-adevăr, dacă $(j, i_p) \in G$, atunci, din egalitatea $(i_1, j) = (i_1, i_p)(j, i_p)(i_1, i_p)$, rezultă că $(i_1, j) \in G$, ceea ce contrazice alegerea lui m. Dacă $m = n$, atunci orice transpoziție aparține lui G. Cum orice permutare este un produs de transpoziții, rezultă că $G = \sigma_n$.

Presupunem acum că $m < n$. Există atunci j_1 cu $1 \leqslant j_1 \leqslant n$ și $j_1 \notin \{i_1, \ldots, i_m.\}$ Cum G este tranzitiv, există $\sigma \in G$ astfel încît $\sigma(i_1) = j_1$. Notăm $\sigma(i_k) = j_k$ $(k = 1, 2, \ldots, m)$. Avem

$$\{i_1, i_2, \ldots, i_m\} \cap \{j_1, \ldots, j_m\} = \emptyset.$$

Într-adevăr, dacă $j_p \in \{i_1, i_2, \ldots, i_m\}$, atunci deoarece $\sigma^{-1}(i_1, i_p)\sigma = (j_2, j_p)$, rezultă că $(j_1, j_p) \in G$, adică se obține o contradicție Deoarece $\{i_1, i_2, \ldots, i_m\} \cap \{j_1, \ldots, j_m\} = \emptyset$, avem $2m \leqslant n$. Dacă $2m < n$, alegem k_1 cu $1 \leqslant k_1 \leqslant n$ și $k_1 \notin \{i_1, \ldots, i_m\} \cap \{j_1, \ldots, j_m\}$. Cum G este tranzitiv, există $\tau \in G$ astfel încît $\tau(i_1) = k_1$. Punem $\tau(i_\alpha) = k_\alpha$, $\alpha = 1, 2, \ldots, m$. Analog, ca mai sus, se arată

$$\{k_1, \ldots, k_m\} \cap \{i_1, \ldots, i_m\} = \emptyset \text{ și } \{k_1, \ldots, k_m\} \cap \{j_1, \ldots, j_m\} = \emptyset.$$

Rezultă că $3m \leqslant n$. Continuînd raționamentul se obține că există 1, număr natural, astfel încît $n = lm$ și deci n nu este număr prim. Deci, trebuie că $m = n$ și atunci $G = \sigma_n$.

Teorema 11.3. *Fie K un corp astfel încît $K \subseteq \mathbb{R}$. Fie $f \in K[X]$ un polinom ireductibil cu grad $f = p$, p fiind număr prim. Dacă f are numai două rădăcini complexe, atunci grupul lui Galois G al lui f este izomorf cu σ_p.*

Demonstrație. Fie $\alpha_1, \alpha_2, \ldots, \alpha_p$ rădăcinile lui f. Din ipoteză putem presupune că α_1, α_2 sînt complexe iar $\alpha_3, \ldots, \alpha_p \in \mathbb{R}$. În aceste condiții $\alpha_2 = \bar{\alpha}_1$. Fie E corpul de descompunere al lui f. Atunci $E = K(\alpha_1, \ldots, \alpha_p)$. Punem $G = G(E/K)$ și $X = \{\alpha_1, \ldots, \alpha_p\}$. După propoziția 11.1 rezultă că aplicația $G \xrightarrow{\varphi} S_X$, unde $\varphi(u) = u|X$ este un omomorfism injectiv. Să arătăm că φ este și surjectivă. Să notăm $H = \operatorname{Im} \varphi \subseteq S_X$ și să arătăm că H este tranzitiv pe mulțimea X. Pentru aceasta, fie $\alpha_i, \alpha_j \in X$.

Din teorema elementelor conjugate există $u \in G(E/K)$ astfel încît $u(\alpha_i) = \alpha_j$ şi deci H este tranzitiv.

Fie $\varepsilon : \mathbb{C} \to \mathbb{C}$, $\varepsilon(a + ib) = a - ib$; ε este un automorfism al lui $\mathbb{C}$. Fie $v = \varepsilon|E$. Atunci $v(\alpha_1) = \alpha_2$, $v(\alpha_2) = \alpha_1$ şi $v(\alpha_i) = \alpha_i$ pentru $i > 2$. Atunci aplicaţia $\varphi(v) = v|X$ este o transpoziţie. După propoziţia 11.2 rezultă că $H = S_X$. Dar $S_X \simeq \sigma_p$ şi deci $G \simeq \sigma_p$.

Teorema 11.4. *Pentru orice număr prim $p \geqslant 5$ există un polinom cu coeficienţi raţionali de grad egal cu p al cărui grup Galois este izomorf cu σ_p.*

Demonstraţie. Fie m un număr întreg par cu $m > 0$. Fie $n_1 < n_2 < \ldots < n_{k-2}$ $k - 2$ numere întregi pare, unde k este număr întreg impar cu $k > 3$. Fie polinomul

$$f(X) = (X^2 + m)(X - n_1)(X - n_2) \ldots (X - n_{k-2}).$$

Polinomul $f(X)$ are $k-2$ rădăcini reale şi anume $n_1, n_2, \ldots, n_{k-2}$. Din teorema lui Rolle rezultă că $f(X)$ are cel puţin $k - 3$ extreme, din care $\frac{k-3}{2}$ sînt maxime şi $\frac{k-3}{2}$ sînt minime. Cum $m \geqslant 2$ şi $n_1, n_2, \ldots, n_{k-2}$ sînt numere pare, atunci $|g(h)| > 2$, pentru orice h număr întreg impar. Rezultă că valorile lui f în punctele de maxim sînt > 2. Dacă punem $g(X) = f(X) - 2$, atunci $g(X)$ are cel puţin $\frac{k-3}{2}$ maxime şi $\frac{k-3}{2}$ minime. În plus, valorile funcţiei $g(X)$ în punctele de maxim sînt > 0. Deoarece sînt $\frac{k-3}{2}$ maxime şi $\frac{k-3}{2}$ minime, rezultă că $g(X)$ are cel puţin $k-3$ rădăcini reale. Cum $g(n_{k-2}) = -f(n_{k-2}) - 2 = -2$ şi $g(+\infty) = +\infty$, rezultă că g mai are o rădăcină reală $> n_{k-2}$. Deci g are cel puţin $k - 2$ rădăcini reale. Vom dovedi acum că pentru m suficient de mare g are două rădăcini complexe.

Fie $g = \prod_{i=1}^{k} (X - x_i)$ descompunerea lui g în $\mathbb{C}[X]$. Deoarece $g(X) = (X^2 + m)(X - n_1) \ldots (X - n_{k-2}) - 2$, atunci, din identificarea coeficienţilor, obţinem

$$\sum_{i=1}^{k} x_i = \sum_{j=1}^{k-2} n_j ; \quad \sum_{i<j} x_i x_j = \sum_{\alpha<\beta} n_\alpha n_\beta + m,$$

iar

$$\sum_{i=1}^{k} x_i^2 = \left(\sum_{i=1}^{k} x_i\right)^2 - 2 \sum_{i<j} x_i x_j = \sum_{\alpha=1}^{k-2} n_\alpha^2 - 2m.$$

Pentru m suficient de mare avem $\sum_{\alpha=1}^{k-2} n_\alpha^2 - 2m < 0$, adică $\sum_{i=1}^{k} x_i^2 < 0$. Înseamnă că cel puțin o rădăcină a polinomului $g(X)$ este complexă. Întrucît $g(X)$ are coeficienți reali, atunci $g(X)$ are cel puțin două rădăcini complexe. Cum grad $g(X) = k$ și $g(X)$ are cel puțin $k - 2$ rădăcini reale, atunci, pentru m suficient de mare, $g(X)$ are $k - 2$ rădăcini reale și două rădăcini complexe.

Polinomul $g(X)$ este ireductibil. Într-adevăr, să scriem $f(X) = X^k + a_1X^{k-2} + \ldots + a_k$, unde $a_1, a_2, \ldots, a_k$ sînt numere pare. Cum $a_k = -mn_1n_2 \ldots n_{k-2}$ și $k > 3$, atunci $4 | a_k$. Atunci $g(X) = f(X) - 2 = X^k + a_1X^{k-2} + \ldots + (a_k - 2)$ are toți coeficienții $a_1, \ldots, a_{k-1}, a_{k-2}$ numere pare. Cum 4 nu divide $a_k - 2$, putem aplica criteriul de ireductibilitate al lui Eisenstein și rezultă că $g(X)$ este un polinom ireductibil de gradul k.

Acum, dacă $k = p$ este număr prim $p \geqslant 5$, rezultă din teorema 11.3 că grupul Galois al polinomului $g(X)$ este izomorf cu σ_p.

VII

REZOLVAREA ECUAȚIILOR ALGEBRICE PRIN RADICALI

§ 1. Grupuri rezolubile

Fie G un grup. Un șir descendent de subgrupuri ale lui G de forma

$$G = H_0 \supset H_1 \supset \ldots \supset H_s = \{e\},$$

cu proprietatea că, pentru orice $1 \leqslant i \leqslant s$, H_i este un subgrup normal în H_{i-1}, se numește *șir normal*. Grupurile factor H_{i-1}/H_i, $1 \leqslant i \leqslant s$, se numesc *factorii șirului*.

Propoziția 1.1. *Fie $\varphi : G \to G'$ un omomorfism surjectiv de grupuri. Dacă $G = H_0 \supset H_1 \supset \ldots \supset H_s = \{e\}$ este un șir normal al lui G, atunci $G' = \varphi(H_0) \supset \varphi(H_1) \supset \ldots \supset \varphi(H_s) = \{e'\}$ este un șir normal al lui G'. În plus, pentru orice $1 \leqslant i \leqslant s$ există un omomorfism surjectiv :*

$$\varphi_i : H_{i-1}/H_i \to \varphi(H_{i-1})/\varphi(H_i).$$

Demonstrație. Fie $y_1, y_2, \in \varphi(H_i)$. Atunci $y_1 = \varphi(x_1)$ și $y_2 = \varphi(x_2)$ cu $x_1, x_2 \in H_i$, iar $y_1y_2^{-1} = \varphi(x_1)\varphi(x_2)^{-1} = \varphi(x_1)\,\varphi(x_2^{-1}) = \varphi(x_1x_2^{-1})$. Deoarece H_i este subgrup, atunci $x_1x_2^{-1} \in H_i$. Deci $y_1y_2^{-1} \in \varphi(H_i)$, ceea ce înseamnă că $\varphi(H_i)$ este subgrup în G'. Să arătăm că $\varphi(H_i)$ este subgrup normal în $\varphi(H_{i-1})$. Fie $y \in \varphi(H_{i-1})$ și $h' \in \varphi(H_i)$. Putem scrie $y = \varphi(x)$ cu $x \in H_{i-1}$ și $h' = \varphi(h)$ cu $h \in H_i$. Atunci $yh'y^{-1} = \varphi(x)\,\varphi(h)\,\varphi(x)^{-1} = \varphi(xhx^{-1})$. Deoarece H_i

este subgrup normal în H_{i-1}, rezultă $xhx^{-1} \in H_i$ şi deci $yh'y^{-1} \in \varphi(H_i)$, ceea ce înseamnă că $\varphi(H_i)$ este subgrup normal în $\varphi(H_{i-1})$. Cum φ este surjectivă, atunci $G' = \varphi(G) = \varphi(H_0)$. Deci $G' = \varphi(H_0) \supset \varphi(H_1) \supset \ldots \supset \varphi(H_s)$ este un şir normal al lui G'.

Definim

$$\varphi_i : H_{i-1}/H_i \to \varphi(H_{i-1})/\varphi(H_i),$$

$$\varphi_i(\hat{x}) = \widehat{\varphi(x)}.$$

Se vede că φ_i este bine definită şi că este omomorfism de grupuri.

Fie $\hat{\hat{y}} \in \varphi(H_{i-1})/\varphi(H_i)$ un element arbitrar. Cum $y \in \varphi(H_{i-1})$, atunci $y = \varphi(x)$ cu $x \in H_{i-1}$. Este clar că $\varphi_i(\hat{x}) = \hat{\hat{y}}$ şi deci φ_i este surjectivă.

Propoziţia 1.2. *Fie* $\varphi : H \to G$ *un morfism de grupuri. Dacă* $G = H_0 \supset H_1 \supset \ldots \supset H_s = \{e\}$ *este un şir normal al lui* G, *atunci*

$$H = \varphi^{-1}(H_0) \supset \varphi^{-1}(H_1) \supset \ldots \supset \varphi^{-1}(H_s) = \{e\}$$

este un şir normal al lui H. *În plus, pentru orice* $1 \leqslant i \leqslant s$, *există un omomorfism injectiv*

$$\varphi_i : \varphi^{-1}(H_{i-1})/\varphi^{-1}(H_i) \to H_{i-1}/H_i.$$

Demonstraţie. Fie $x_1, x_2 \in \varphi^{-1}(H_i)$. Atunci $\varphi(x_1), \varphi(x_2) \in H_i$. Deci $\varphi(x_1) \cdot \varphi(x_2)^{-1} \in H_i$ sau, altfel scris, $\varphi(x_1x_2^{-1}) \in H_i$, de unde rezultă că $x_1x_2^{-1} \in \varphi^{-1}(H_i)$. Deci $\varphi^{-1}(H_i)$ este un subgrup al lui H. Să arătăm că $\varphi^{-1}(H_i)$ este subgrup normal în $\varphi^{-1}(H_{i-1})$. Fie pentru aceasta $h \in \varphi^{-1}(H_i)$ şi $x \in \varphi^{-1}(H_{i-1})$. Deoarece $\varphi(xhx^{-1}) = \varphi(x)\,\varphi(h)\,\varphi(x)^{-1}$ şi H_i este normal în H_{i-1}, rezultă că $\varphi(xhx^{-1}) \in H_i$, de unde $xhx^{-1} \in \varphi^{-1}(H_i)$ şi, prin urmare, $\varphi^{-1}(H_i)$ este subgrup normal în $\varphi^{-1}(H_{i-1})$. Deci, şirul $H = \varphi^{-1}(H_0) \supset \varphi^{-1}(H_1) \supset \ldots \supset \varphi^{-1}(H_s) = \{e\}$ este un şir normal în H.

Definim

$$\varphi_i : \varphi^{-1}(H_{i-1})/\varphi^{-1}(H_i) \to H_{i-1}/H_i,$$

$$\varphi_i(\hat{x}) = \widehat{\varphi(x)},$$

φ_i este un omomorfism de grupuri.

Fie $\hat{x} \in \text{Ker } \varphi_i$; atunci, $\varphi_i(\hat{x}) = \hat{e}$ şi deci $\varphi(x) \in H_i$, de unde rezultă că $x \in \varphi^{-1}(H_i)$. Atunci $\hat{x} = \hat{e}$ şi $\text{Ker } \varphi_i = \{\hat{e}\}$; prin urmare, φ_i este injectiv.

Un grup G se numeşte *rezolubil* dacă el admite un şir normal $G = H_0 \supset H_1 \supset H_2 \supset \ldots \supset H_s = \{e\}$ în care toţi factorii şirului sînt grupuri abeliene.

Teorema 1.3. *Fie G un grup şi H un subgrup normal al lui G. Atunci G este rezolubil dacă şi numai dacă H şi G/H sînt rezolubile.*

Demonstraţie. Dacă G este rezolubil, din propoziţiile 1.1 şi 1.2, rezultă că H şi H/G sînt rezolubile. Reciproc, presupunem că H şi G/H sînt rezolubile. Atunci există pentru H un şir normal $H = H_0 \supset H_1 \supset \ldots \supset H_s = \{e\}$ cu H_{i-1}/H_i abeliene $(1 \leqslant i \leqslant s)$, iar în G/H există un şir normal $G/H = K_0 \supset K_1 \supset \ldots$ $\ldots \supset K_r = \{\hat{e}\}$ cu K_{j-1}/K_j abeliene $(1 \leqslant j \leqslant r)$. Fie $\pi : G \to G/H$ surjecţia canonică. Notăm $L_j = \pi^{-1}(K_j)$, $j = 0, \ldots, r$. Omomorfismul π defineşte un izomorfism între K_{j-1}/K_j şi L_{j-1}/L_j, pentru orice $j = 1, \ldots, r$. Rezultă că L_{j-1}/L_j sînt grupuri abeliene. Atunci următorul şir normal:

$$G = L_0 \supset L_1 \supset \ldots \supset L_r = H = H_0 \supset \ldots \supset H_s = \{e\}$$

are toţi factorii şirului grupuri abeliene. Deci G este rezolubil.

Exemple. 1. Orice grup abelian G este rezolubil.

2. Fie A un inel comutativ unitar. Notăm cu $U(A)$ mulţimea elementelor inversabile din A. Atunci $U(A)$ este grup abelian faţă de operaţia de înmulţire din inelul A.

Notăm $M(A) = U(A) \times A$. Pe $M(A)$ definim operaţia $*$ în felul următor: fie (a, b) şi (c, d) două elemente din $M(A)$; atunci

$$(a, b) * (c, d) = (ac, bc + d).$$

Se verifică uşor că operaţia $*$ este asociativă. Elementul $(1, 0)$ este element neutru în $M(A)$ iar dacă $(a, b) \in M(A)$, atunci (a^{-1}, ba^{-1}) este inversul său. Deci $M(A)$ este un grup (în general neabelian).

Definim aplicaţia

$$\varphi : M(A) \to U(A), \quad \varphi(a, b) = a.$$

Aplicaţia φ este omomorfism surjectiv de grupuri şi

$$\text{Ker } \varphi = \{(a, b) \mid \varphi(a, b) = 1\} = \{(a, b) \in M(A) \mid a = 1\} = \{(1, b) \mid b \in A\}.$$

Se vede ușor că Ker φ este izomorf cu grupul abelian subiacent structurii de inel a lui A. Din teorema 1.3 rezultă că $M(A)$ este un grup rezolubil. Să considerăm un caz particular. Fie inelul $A = \mathbb{Z}_n$. Atunci

$$U(\mathbb{Z}_n) = \mathbb{Z}_n^* = \{\hat{a} \mid (a, n) = 1\}.$$

Notăm $M_n = M(\mathbb{Z}_n) = \mathbb{Z}_n^* \times \mathbb{Z}_n$.

Se observă că M_n este un grup finit rezolubil. Ordinul său este egal cu $n \cdot \varphi(n)$, unde $\varphi(n)$ este indicatorul lui Euler al numărului natural n.

3. Grupurile simetrice $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ sînt rezolubile. Într-adevăr, considerăm grupul altern A_n. Acesta este un subgrup normal în σ_n și $\sigma_n/A_n \simeq \{-1, 1\}$. Grupul A_n are $\frac{n!}{2}$ elemente. Să studiem grupurile A_n, pentru $n = 1, 2, 3, 4$. Astfel, pentru $n = 1$, $A_1 = \{e\}$; pentru $n = 2$, $A_2 = \{e\}$.

Dacă $n=3$ A_3 este ciclic (are trei elemente) și deci abelian. Rezultă că $\sigma_1, \sigma_2, \sigma_3$ sînt rezolubile.

Pentru $n = 4$, A_4 are 12 elemente.

Considerăm în A_4 elementele

$$H = \{e, t_1 = (1, 2)(3, 4), t_2 = (1, 3)(2, 4), t_3 = (1, 4)(2, 3)\}.$$

Este evident că $H \subseteq A_4$. Au loc relațiile:

$$t_1^2 = t_2^2 = t_3^2 = e; \quad t_1t_2 = t_2t_1 = t_3, \ t_1t_3 = t_3t_1 = t_2 \text{ și } t_2t_3 = t_3t_2 = t_1.$$

Deci H este un subgrup al lui A_4. De asemenea, H este abelian și este un subgrup normal în σ_4. Într-adevăr, vom arăta că $at_ia^{-1} \in H$, pentru orice $a \in \sigma_4$ și $i = 1, 2, 3$. Cum a este un produs de transpoziții este suficient să considerăm cazul cînd a este o transpoziție:

$$\begin{array}{llll}
a = (1, 2) & (1, 2)\,t_1(1, 2) = t_1; & (1, 2)\,t_2(1, 2) = t_3; & (1, 2)\,t_3(1, 2) = t_2, \\
a = (1, 3) & (1, 3)\,t_1(1, 3) = t_3; & (1, 3)\,t_2(1, 3) = t_2; & (1, 3)\,t_3(1, 3) = t_1, \\
a = (1, 4) & (1, 4)\,t_1(1, 4) = t_2; & (1, 4)\,t_2(1, 4) = t_1; & (1, 4)\,t_3(1, 4) = t_3, \\
a = (2, 3) & (2, 3)\,t_1(2, 3) = t_2; & (2, 3)\,t_2(2, 3) = t_1; & (2, 3)\,t_3(2, 3) = t_3, \\
a = (2, 4) & (2, 4)\,t_1(2, 4) = t_3; & (2, 4)\,t_2(2, 4) = t_2; & (2, 4)\,t_3(2, 4) = t_1, \\
a = (3, 4) & (3, 4)\,t_1(3, 4) = t_1; & (3, 4)\,t_2(3, 4) = t_3; & (3, 4)\,t_3(3, 4) = t_2.
\end{array}$$

Deoarece A_4/H are trei elemente, înseamnă că este grup ciclic, deci abelian. Atunci A_4 este grup rezolubil. Întrucît σ_4/A_4 este izomorf cu grupul $\{-1, 1\}$ cu operația de înmulțire, din teorema 1.3 rezultă că σ_4 este rezolubil.

§ 2. Grupul A_n $(n \geqslant 5)$

Un grup G se numește *simplu* dacă singurele sale subgrupuri normale sînt $\{e\}$ și G.

Teorema 2.1. *Dacă $n \geqslant 5$, grupul A_n este simplu.*

Demonstrație. Fie $H \subseteq A_n$ un subgrup normal diferit de $\{e\}$. Vom arăta că $H = A_n$. Există $\sigma \in H$, $\sigma \neq e$. Scriem pe σ ca un produs de cicluri disjuncte. Această scriere poate să aibă una din următoarele patru forme :

1) $\sigma = (i_0, i_1, i_2, i_3, \ldots)(\quad)(\quad)\ldots,$

adică cel puțin un ciclu are lungimea 4 ;

2) $\sigma = (i_0, i_1, i_2)(i_3, i_4, \ldots)(\quad)\ldots;$

3) $\sigma = (i_0, i_1, i_2);$

4) $\sigma = (i_0, i_1)(i_2, i_3)\ldots$

produs de transpoziții disjuncte (în număr par).

La fiecare situație în parte asociem permutările :

1') $\tau = (i_1, i_2, i_3) = (i_1, i_3)(i_2, i_3),$

2') $\tau = (i_1, i_2, i_4) = (i_1, i_4)(i_2, i_4),$

3') $\tau = (i_1, i_2, i_3) = (i_1, i_3)(i_2, i_3),$

4') $\tau = (i_1, i_2, i_3) = (i_1, i_3)(i_2, i_3).$

Se vede că în fiecare situație $\tau \in A_n$.

Notăm $t = \tau\sigma\tau^{-1}\sigma^{-1}$, $t \in H$ (deoarece H este subgrup normal). Să calculăm pe t:

1) + 1') = 1'') $t = (i_0, i_2, i_3)$

2) + 2') = 2'') $t = (i_0, i_3, i_1, i_2, i_4)$

3) + 3') = 3'') $t = (i_0, i_3)(i_1, i_2)$

4) + 4') = 4'') $t = (i_0, i_2)(i_1, i_3)$

Deci, dacă σ este de forma 3) sau 4), atunci H conține produsul a două transpoziții disjuncte.

Presupunem că σ este de forma 1). Din 1'') se vede că H conține o permutare de forma 3) și din 3'') rezultă că H conține produsul a două transpoziții disjuncte.

Dacă σ este de forma 2), atunci din 2'') rezultă că H conține o permutare de forma 1) și deci H conține produsul a două transpoziții disjuncte. Deci, am verificat că H conține produsul a două transpoziții disjuncte. Fie $(j_1, j_2)(j_3, j_4)$ un produs de

două transpoziţii disjuncte ce aparţin lui H. Fie $(k_1, k_2)(k_3, k_4)$ produsul arbitrar a două transpoziţii disjuncte. Considerăm permutarea

$$a = \begin{pmatrix} \dots k_1 \dots k_2 \dots k_3 \dots k_4 \dots \\ \dots j_1 \dots j_2 \dots j_3 \dots j_4 \dots \end{pmatrix}$$

care există. Are loc egalitatea

$$a(j_1, j_2)(j_3, j_4)a^{-1} = (k_1, k_2)(k_3, k_4).$$

Notăm $b = a(j_1, j_2)$. Atunci

$$b(j_1, j_2)(j_3, j_4)b^{-1} = a(j_1, j_2)(j_1, j_2)(j_3, j_4)(j_1, j_2)^{-1}a^{-1} =$$

$$= a(j_3, j_4)(j_1, j_2)a^{-1} = a(j_1, j_2)(j_3, j_4)a^{-1} = (k_1, k_2)(k_3, k_4).$$

Dacă a este o permutare pară, atunci din $a \in A_n$ rezultă că şi $a(j_1, j_2)(j_3, j_4)a^{-1} \in H$, deci $(k_1, k_2)(k_3, k_4) \in H$.

Dacă a este impară, atunci b este o permutare pară şi $b(j_1, j_2)(j_3, j_4)b^{-1} \in H$, deci $(k_1, k_2)(k_3, k_4) \in H$. Astfel orice produs a două transpoziţii disjuncte aparţine lui H.

Vom dovedi că H conţine produsul oricăror două transpoziţii. Mai precis, vom arăta că $(j_1, j_2)(j_1, j_3) \in H$, unde j_1, j_2, j_3 sînt distincte. Deoarece $n \geqslant 5$, există $l_1, l_2 \in \{1, 2, \dots, n\}$ distincte astfel încît

$$\{l_1, l_2\} \cap \{j_1, j_2, j_3\} = \emptyset.$$

Conform celor demonstrate mai sus avem

$$(l_1, l_2)(j_1, j_2) \in H \quad \text{şi} \quad (l_1, l_2)(j_1, j_3) \in H.$$

Rezultă

$$(l_1, l_2)(j_1, j_2)(l_1, l_2)(j_1, j_3) = (l_1, l_2)(l_1, l_2)(j_1, j_2)(j_1, j_3) =$$

$$= (j_1, j_2)(j_1, j_3),$$

de unde se obţine $(j_1, j_2)(j_1, j_3) \in H$. Cum orice permutare $\sigma \in A_n$, $\sigma \neq e$, este un produs par de transpoziţii, rezultă că $\sigma \in H$. Deci $H = A_n$.

Corolarul 2.2. *Pentru* $n \geq 5$ *grupurile* A_n și σ_n *nu sînt rezolubile.*

Demonstrație. Dacă A_n ar fi rezolubil, atunci ar exista un șir normal de forma

$$A_n = H_0 \supset H_1 \supset \ldots \supset H_s = \{e\},$$

unde H_{i-1}/H_i sînt grupuri abeliene ($1 \leq i \leq s$).

Fie k primul număr natural pentru care $A_n \neq H_k$. Atunci H_k este subgrup normal în A_n și aplicînd teorema 2.1 rezultă că $H_k = \{e\}$. Deoarece $H_{k-1} = A_n$ și H_{k-1}/H_k este abelian, rezultă că A_n este abelian, ceea ce reprezintă o contradicție. Dacă A_n nu este rezolubil, atunci și σ_n nu este rezolubil.

§ 3. Extinderi radicale simple

Fie K un corp și E o extindere a lui K. Extinderea E se numește *radicală simplă* dacă E este corp de descompunere al unui polinom de forma

$$x^n - a, \quad a \in K.$$

Ne propunem să calculăm grupul Galois al acestei extinderi.

Teorema 3.1. *Fie* $K \subset E$ *o extindere radicală simplă dată de polinomul* $X^n - a$, $a \in K$. *Dacă* G *este grupul Galois* $G(E/K)$, *atunci există un morfism injectiv*

$$\varphi : G \to M_n \quad (M_n = \mathbb{Z}_n^* \times \mathbb{Z}_n).$$

În particular, rezultă că grupul Galois $G(E/K)$ *este rezolubil.*

Demonstrație. Fie ξ o rădăcină primitivă a ecuației $x^n - 1 = 0$. Fie θ o rădăcină arbitrară a ecuației

$$x^n - a = 0.$$

Atunci, mulțimea rădăcinilor acestei ecuații este

$$\{\theta, \xi\theta, \ldots, \xi^{n-1}\theta\}.$$

Deci $E = K(\theta, \xi\theta, \ldots, \xi^{n-1}\theta) = K(\xi, \theta)$.

Fie $\sigma \in G = G(E/K)$. Deoarece $\xi^n = 1$, atunci $\sigma(\xi)^n = 1$, adică $\sigma(\xi)$ este o rădăcină de ordinul n a unității. Există deci un număr natural r astfel încît

$$\sigma(\xi) = \xi^r.$$

Dacă $\theta^n = a$, atunci $\sigma(\theta)^n = \sigma(a) = a$. Deci există un număr natural s astfel încît $\sigma(\theta) = \xi^s\theta$. Numărul r este prim cu n. Într-adevăr, dacă r și n nu sînt prime, fie d cel mai mare divizor comun al lui r și n. Atunci $r = dr'$ și $n = dn'$. Deci $\sigma(\xi)^{n'} = (\xi^r)^{n'} = \xi^{dr'n'} = (\xi^n)^{r'} = 1$, de unde rezultă $\sigma(\xi^{n'}) = \sigma(1)$ și deci $\xi^{n'} = 1$, ceea ce înseamnă că ξ este o rădăcină de ordinul n' a unității. Cum $n' < n$, obținem o contradicție. Deci, trebuie ca r și n să fie prime între ele. Definim

$$\varphi : G \to M_n = \mathbb{Z}_n^* \times \mathbb{Z}_n, \ \varphi(\sigma) = (\hat{r}, \hat{s}).$$

Să dovedim că φ este omomorfism de grupuri. Fie $\sigma, \tau \in G$ și fie

$$\varphi(\sigma) = (\hat{r}, \hat{s}), \ \varphi(\tau) = (\hat{t}, \hat{u}).$$

Deci

$$\sigma(\xi) = \xi^r, \ \sigma(\theta) = \xi^s\theta,$$

$$\tau(\xi) = \xi^t, \ \tau(\theta) = \xi^u\theta.$$

Atunci

$$(\sigma\tau)(\xi) = \sigma(\tau(\xi)) = \sigma(\xi^t) = \sigma(\xi)^t = \xi^{rt}$$

și

$$(\sigma\tau)(\theta) = \sigma(\tau(\theta)) = \sigma(\xi^u\theta) = \sigma(\xi)^u\,\sigma(\theta) = \xi^{ru}\xi^s\theta = \xi^{ru+s}\theta.$$

Deci $\varphi(\sigma \circ \tau) = (\widehat{rt}, \widehat{ru + s}) = (\hat{r}, \hat{s})(\hat{u}, \hat{t})$, adică φ este un omomorfism de grupuri. Dacă $\varphi(\sigma) = (\hat{1}, \hat{0})$, atunci $(\hat{r}, \hat{s}) = (\hat{1}, \hat{0})$. Deci n divide pe $r - 1$ și n divide s. Rezultă că $r - 1 = nm$ și $s = nn'$. Cum $\sigma(\xi) = \xi^r$, atunci $\sigma(\xi) = \xi^{nm+1} = \xi$. De asemenea, $\sigma(\theta) = \xi^s\theta = \xi^{nn'}\theta = \theta$. Din egalitățile $\sigma(\xi) = \xi$ și $\sigma(\theta) = \theta$ și din faptul că $E = K(\xi, \theta)$ rezultă imediat că $\sigma = 1_E$. Deci φ este injectivă.

Corolarul 3.2. *Fie K un corp, E o extindere radicală simplă a lui K dată de polinomul $X^n - a$, $a \in K$. Dacă corpul K conține o rădăcină primitivă a unității de ordinul n, atunci grupul $G(E/K)$ este ciclic. Dacă în plus $X^n - a$ este ireductibil în $K[X]$, atunci $G(E/K) \simeq \mathbb{Z}_n$.*

Demonstrație. Fie $E = K(\xi, \theta)$. Dacă $\xi \in K$, atunci $E = K(\theta)$. Fie σ un element din $G(E/K)$. Atunci

$$\sigma(\theta) = \xi^r \theta.$$

Definim $\psi : G \to \mathbb{Z}_n$, $\psi(\sigma) = \hat{r}$. Dacă $\sigma, \tau \in G$, să arătăm că $\psi(\sigma \circ \tau) = \psi(\sigma) + \psi(\tau)$.

Într-adevăr, dacă

$$\sigma(\theta) = \xi^r \theta \text{ și } \tau(\theta) = \xi^s \theta,$$

atunci

$$(\sigma \circ \tau)(\theta) = \sigma(\tau(\theta)) = \sigma(\xi^s \theta) = \xi^s \sigma(\theta) = \xi^{r+s} \theta,$$

de unde rezultă

$$\psi(\sigma \circ \tau) = \widehat{r+s} = \hat{r} + \hat{s} = \psi(\sigma) + \psi(\tau).$$

Deci ψ este omomorfism de grupuri.

Dacă $\psi(\sigma) = \hat{0}$, atunci n divide pe r. Cum $\sigma(\theta) = \xi^r \theta$, rezultă că $\xi^r = 1$ și deci $\sigma(\theta) = \theta$. Dar $E = K(\theta)$, deci $\sigma = 1_E$. Astfel ψ este injectivă. Rezultă că $G(E/K)$ este ciclic. Dacă $X^n - a$ este ireductibil, atunci ord $G = n$. Cum $\mathbb{Z}_n$ are n elemente, rezultă că ψ este și surjectivă.

Deci $G = G(E/K) \simeq \mathbb{Z}_n$.

Teorema 3.3 (*reciproca corolarului* 3.2). *Fie K un corp și E o extindere normală a lui K. Presupunem că $G = G(E/K)$ este grup ciclic de ordinul n, iar K conține o rădăcină primitivă de ordinul n a unității. Atunci există un polinom $X^n - a$, $a \in K$, astfel încît E este corpul de descompunere al acestui polinom.*

Demonstrație. Notăm cu ξ o rădăcină primitivă a unității. Deci $\xi \in K$. Cum G este ciclic de ordinul n, putem scrie

$$G = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}.$$

Fie $\alpha \in E$ şi $p \in \mathbb{Z}$. Considerăm elementul $(\xi^p, \alpha) = \alpha + \xi^p \sigma(\alpha) + \xi^{2p}\sigma^2(\alpha) + \ldots + \xi^{p(n-1)}\sigma^{n-1}(\alpha)$. Acest element se numeşte *p-rezolventa lui Lagrange* asociată elementului α.

Etapa întîi. Dacă $(\xi, \alpha) \neq 0$, atunci $K(\alpha) = E$. Presupunem prin reducere la absurd că $K(\alpha) \neq E$. Notăm $H = G(E/K(\alpha))$. Dacă G este ciclic, atunci H este ciclic. Presupunem că H este generat de σ^d, $0 \leqslant d \leqslant n-1$. Atunci ord $H = m = \dfrac{n}{d}$. Putem scrie

$$(\xi, \alpha) = \sum_{k=0}^{n-1} \xi^k \sigma^k(\alpha) = \sum_{i=0}^{m-1}\sum_{j=0}^{d-1} \xi^{id+j}\sigma^{id+j}(\alpha),$$

unde $k = id + j$ cu $0 \leqslant j \leqslant d - 1$ şi $0 \leqslant i \leqslant m - 1$

$$(\xi, \alpha) = \sum_{j=0}^{d-1}\sum_{i=0}^{m-1} \xi^{id}\xi^j\sigma^{id}\,(\sigma^j(\alpha)) = \sum_{j=0}^{d-1}\sum_{i=0}^{m-1} \xi^{id}\xi^j\sigma^j(\sigma^{id}(\alpha)).$$

Dacă $\sigma^d \in H$, atunci $\sigma^{id}(\alpha) = \alpha$. Deci

$$(\xi, \alpha) = \sum_{j=0}^{d-1} \xi^{ij} \sum_{i=0}^{m-1} \xi^{id}\sigma^j(\alpha) = \sum_{j=0}^{d-1} \xi^j\sigma^j(\alpha) \sum_{i=0}^{m-1} \xi^{id}.$$

Dar $\displaystyle\sum_{i=0}^{m-1} \xi^{id} = \frac{1 - \xi^{md}}{1 - \xi^d} = \frac{1 - \xi^n}{1 - \xi^d} = 0$, deci $(\xi, \alpha) = 0$,

ceea ce reprezintă o contradicţie.

Etapa a doua. Vom arăta că există $\alpha \in E$ astfel încît $(\xi, \alpha) \neq 0$. Presupunem că, oricare ar fi $\alpha \in E$, avem $(\xi, \alpha) = 0$. Cum E este o extindere finită a lui K, există $\theta \in E$ astfel încît $E = K(\theta)$. Dacă f este polinomul minimal al lui θ, atunci grad $f = n$. Dar θ este rădăcină a lui f, atunci şi $\sigma(\theta)$, $\sigma^2(\theta)$, $\ldots$, $\sigma^{n-1}(\theta)$ sînt rădăcini ale lui f. Să considerăm mulţimea

$$\{\theta, \sigma(\theta), \sigma^2(\theta), \ldots, \sigma^{n-1}(\theta)\}.$$

Elementele acestei mulţimi sînt distincte între ele, deoarece în caz contrar, dacă $\sigma^i(\theta) = \sigma^j(\theta)$ şi $E = K(\theta)$, rezultă $\sigma^i = \sigma^j$, ceea ce reprezintă o contradicţie.

Avem $(\xi, 1) = (\xi, \theta) = (\xi, \theta^2) = \ldots = (\xi, \theta^{n-1}) = 0$, de unde se obțin egalitățile

$$(\xi, 1) = 1 + \xi + \xi^2 + \ldots + \xi^{n-1} = 0,$$

$$(\xi, \theta) = \theta + \xi\sigma(\theta) + \ldots + \xi^{n-1}\sigma^{n-1}(\theta) = 0,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(\xi, \theta^{n-1}) = \theta^{n-1} + \xi\sigma(\theta^{n-1}) + \ldots + \xi^{n-1}\sigma^{n-1}(\theta^{n-1}) = 0.$$

Asociem sistemul de ecuații

$$\left.\begin{array}{l} X_1 + X_2 + \ldots + X_n = 0 \\ \theta X_1 + \sigma(\theta)X_2 + \ldots + \sigma^{n-1}(\theta)\, X_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \theta^{n-1}X_1 + \sigma(\theta^{n-1})X_2 + \ldots + \sigma^{n-1}(\theta^{n-1})X_n = 0 \end{array}\right\}$$

Cum $(1, \xi, \xi^2, \ldots, \xi^{n-1})$ este o soluție a acestui sistem, înseamnă că

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \theta & \sigma(\theta) & \ldots & \sigma^{n-1}(\theta) \\ \ldots & \ldots & \ldots & \ldots \\ \theta^{n-1} & \sigma(\theta^{n-1}) & \ldots & \sigma^{n-1}(\theta^{n-1}) \end{vmatrix} = 0.$$

Notăm $a_1 = \theta$, $a_2 = \sigma(\theta)$, $\ldots$, $a_n = \sigma^{n-1}(\theta)$. Atunci avem

$$\begin{vmatrix} 1 & 1 & \ldots 1 \\ a_1 & a_2 & \ldots a_n \\ a_1^2 & a_2^2 & \ldots a_n^2 \\ \ldots & \ldots & \ldots \\ a_1^{n-1} & a_2^{n-1} & \ldots a_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (a_i - a_j) = 0,$$

de unde rezultă că există $i \neq j$ astfel încît $a_i = a_j$, adică f are două rădăcini egale. Deci se obține o contradicție. Așadar, trebuie să existe $\alpha \in E$ astfel încît $(\xi, \alpha) \neq 0$.

E t a p a a t r e i a. Fie $\alpha \in E$ un element pentru care $(\xi, \alpha) \neq 0$. Dacă notăm $\bar{\alpha} = (\xi, \alpha)$, să arătăm că $K(\bar{\alpha}) = E$ şi $\bar{\alpha}^n \in K$. Într-adevăr, din egalitatea

$$(\xi^p, \alpha) = \alpha + \xi^p \sigma(\alpha) + \ldots + \xi^{p(n-1)} \sigma^{n-1}(\alpha)$$

obţinem

$$\sigma(\xi^p, \alpha) = \sigma(\alpha) + \xi^p \sigma^2(\alpha) + \ldots + \xi^{p(n-1)} \sigma^n(\alpha) =$$

$$= \sigma(\alpha) + \xi^p \sigma^2(\alpha) + \ldots + \xi^{p(n-1)} \alpha = \xi^{-p}(\xi^p, \alpha).$$

Dacă facem $p = 1$, obţinem

$$\sigma(\xi, \alpha) = \xi^{-1}(\xi, \alpha),$$

de unde, prin ridicare la puterea p, obţinem

$$\sigma((\xi, \alpha)^p) = \xi^{-p}(\xi, \alpha)^p$$

şi prin împărţire cu egalitatea $\sigma(\xi^p, \alpha) = \xi^{-p}(\xi^p, \alpha)$, obţinem

$$\sigma\left(\frac{(\xi^p, \alpha)}{(\xi, \alpha)^p}\right) = \frac{(\xi^p, \alpha)}{(\xi, \alpha)^p}.$$

Notăm $c_p = \dfrac{(\xi^p, \alpha)}{(\xi, \alpha)^p}$. Deoarece $\sigma(c_p) = c_p$, atunci $c_p \in K$. Deci avem $(\xi^p, \alpha) = c_p(\xi, \alpha)^p$. Dacă facem $p = n$, obţinem $(\xi^n, \alpha) = c_n(\xi, \alpha)^n$ sau $(1, \alpha) = c_n(\xi, \alpha)^n$. Dar $(1, \alpha) = \alpha + \sigma(\alpha) + \sigma^2(\alpha) + \ldots + \sigma^{n-1}(\alpha)$. Cum $\sigma((1, \alpha)) = \sigma(\alpha) + \sigma^2(\alpha) + \sigma^3(\alpha) + \ldots + \sigma^n(\alpha) = \sigma(\alpha) + \sigma^2(\alpha) + \ldots + \sigma^{n-1}(\alpha) + \alpha = (1, \alpha)$, rezultă că $(1, \alpha) \in K$. Din egalitatea $(1, \alpha) = c_n \bar{\alpha}^n$ rezultă că $\bar{\alpha}^n \in K$. Să arătăm acum că $K(\bar{\alpha}) = E$. Din etapa întîi avem $K(\tilde{\ }) = E$. Din egalităţile

$$(\xi^p, \alpha) = \sum_{k=0}^{n-1} \xi^{pk} \sigma^k(\alpha), \quad p = 0, 1, \ldots, n-1,$$

obţinem

$$\sum_{p=0}^{n-1} (\xi^p, \alpha) = \sum_{p=0}^{n-1} \sum_{k=0}^{n-1} \xi^{pk} \sigma^k(\alpha) = \sum_{k=0}^{n-1} \sum_{p=0}^{n-1} \xi^{pk} \sigma^k(\alpha) =$$

$$= \sum_{p=0}^{n-1} \xi^{p\cdot 0}\sigma^0(\alpha) + \sum_{k=1}^{n-1}\sum_{p=0}^{n-1} \xi^{pk}\sigma^k(\alpha) =$$

$$= n\alpha + \sum_{k=1}^{n-1} \sigma^k(\alpha) \sum_{p=0}^{n-1} \xi^{pk} = n\alpha + \sum_{k=1}^{n-1} \sigma^k(\alpha) \cdot \frac{1-\xi^n}{1-\xi^k} = n\alpha.$$

Din $(\xi^p, \alpha) = c_p(\xi, \alpha)^p = c_p\bar{\alpha}^p$ rezultă $n\alpha = \sum_{p=0}^{n-1} c_p\bar{\alpha}^p \in K(\bar{\alpha})$. Deci $\alpha \in K(\bar{\alpha})$, de unde $K(\alpha) \subseteq K(\bar{\alpha})$ şi $E = K(\bar{\alpha})$.

Să trecem acum la *demonstraţia* teoremei.

Fie $\bar{\alpha}$ din etapa a treia. Avem $\bar{\alpha}^n = c_n \in K$ şi $K(\bar{\alpha}) = E$. Să considerăm polinomul $X^n - c_n \in K[X]$. Fie $\bar{\alpha}$ rădăcină a acestui polinom. Cum K conţine o rădăcină primitivă a unităţii de ordinul n şi $K(\bar{\alpha}) = E$, rezultă că E este corpul de descompunere al polinomul $X^n - c_n$.

§ 4. Extinderi radicale

Fie K un corp ; o extindere E a lui K se numeşte *radicală* dacă există şirul de extinderi

$$K = E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_s = E$$

astfel încît E_i să fie o extindere radicală simplă a lui E_{i-1}, pentru orice i, $1 \leqslant i \leqslant s$.

Teorema 4.1. *Fie E o extindere radicală a lui K. Atunci există o extindere L a lui K cu proprietăţile :*

1) *L este o extindere radicală a lui K şi $E \subset L$;*

2) *L este normală.*

Demonstraţie. Există şirul de extinderi

$$K = E_0 \subset E_1 \subset \ldots \subset E_s = E$$

astfel încît E_i este o extindere radicală simplă a lui E_{i-1}. Procedăm prin inducţie după s. Dacă $s = 1$, atunci $E = E_1$ şi cum

E_1 este o extindere radicală simplă a lui K, atunci E_1 este o extindere normală a lui K şi putem lua $L = E_1$.

Presupunem afirmaţia adevărată pentru $s - 1$ şi verificăm pentru s. Deoarece E_{s-1} este o extindere radicală a lui K, atunci există o extindere normală F a lui K astfel încît $E_{s-1} \subseteq F$. Cum E_s este o extindere radicală simplă a lui E_{s-1}, există polinomul $X^n - c$, $c \in E_{s-1}$, astfel încît E_s este corpul de descompunere peste E_{s-1} al polinomului $X^n - c$. Putem scrie $E_s = E_{s-1}(\xi, \theta)$, unde ξ este o rădăcină primitivă a unităţii, de ordinul n, iar θ este o rădăcină a polinomului $X^n - c$.

Fie f polinomul minimal al lui c peste K. Să notăm cu $\beta_1, \beta_2, \ldots, \beta_r$ rădăcinile lui f. Presupunem că $\beta_1 = c$. Dacă F este normală peste K, atunci $\beta_1, \beta_2, \ldots, \beta_r \in F$. Pentru fiecare $1 \leqslant i \leqslant r$ considerăm polinoamele $X^n - \beta_i \in F[X]$. Fie α_i o rădăcină a polinomului $X^n - \beta_i$. Pentru polinomul $X^n - \beta_1 = X^n - c$, alegem $\alpha_1 = \theta$. Vom nota

$$L = F(\xi, \alpha_1, \alpha_2, \ldots, \alpha_r).$$

Din $\alpha_1 = \theta$ şi $\xi \in E_s$ rezultă că $E \subseteq L$. Notăm $L_i = F(\xi, \alpha_1, \alpha_2, \ldots, \alpha_i)$, pentru $i \geqslant 1$ şi $L_0 = F$. Se vede că $L_i = L_{i-1}(\alpha_i)$. Cum α_i este rădăcină a lui $X^n - \beta_i$ şi $\xi \in L_{i-1}$, rezultă că L_i este corpul de descompunere peste L_{i-1} al polinomului $X^n - \beta_i$ şi deci L este o extindere radicală a lui F. Deoarece F este o extindere radicală a lui K, rezultă că L este o extindere radicală a lui K. Să considerăm polinomul

$$G(X) = f(X^n) \in K[X].$$

Dacă $f = (X - \beta_1)(X - \beta_2) \ldots (X - \beta_r)$, atunci $G(X) = (X^n - \beta_1)(X^n - \beta_2) \ldots (X^n - \beta_r)$. Dar rădăcinile lui $X^n - \beta_1$ sînt $\alpha_1, \xi\alpha_1, \xi^2\alpha_1, \ldots, \xi^{n-1}\alpha_1$, rădăcinile lui $X^n - \beta_2$ sînt $\alpha_2, \xi\alpha_2, \xi^2\alpha_2, \ldots, \xi^{n-1}\alpha_2, \ldots$, rădăcinile lui $X^n - \beta_r$ sînt $\alpha_r, \xi\alpha_r, \xi^2\alpha_r, \ldots, \xi^{n-1}\alpha_r$. Din $L = F(\xi, \alpha_1, \ldots, \alpha_r)$ rezultă că L este corpul de descompunere al lui $G(X)$ peste corpul F. Cum F este normală peste K, există un polinom $h \in K[X]$ astfel încît F este corpul de descompunere al polinomului h peste K. Dar polinomul $h(X) \cdot G(X) \in K[X]$; se vede uşor că L este corpul de descompunere al acestui polinom peste corpul K şi deci L este normală peste K.

Teorema 4.2. *Dacă E este o extindere normală şi radicală a corpului K, atunci grupul $G = G(E/K)$ este rezolubil.*

Demonstrație. Există șirul de extinderi

$$K = E_0 \subset E_1 \subset \dots \subset E_s = E,$$

unde E_i este o extindere radicală simplă a lui E_{i-1} $(1 \leqslant i \leqslant s)$.
Notăm $H_i = G(E/E_i)$ $(0 \leqslant i \leqslant s)$. Atunci $H_0 = G$ și $H_s = G(E/E) = \{e\}$. Obținem șirul descrescător de subgrupuri

$$G = H_0 \supset H_1 \supset \dots \supset H_s = \{e\}.$$

Deoarece E_i este o extindere normală a lui E_{i-1}, se obține

$$G(E_i/E_{i-1}) \simeq H_{i-1}/H_i.$$

Din faptul că E_i este o extindere radicală simplă a lui E_{i-1} rezultă că H_{i-1}/H_i este grup rezolubil $(1 \leqslant i \leqslant s)$. Din $H_s = \{e\}$ rezultă că H_{s-1} este rezolubil. Dacă H_{s-2}/H_{s-1} este rezolubil, aplicînd teorema 1.3, obținem că H_{s-2} este rezolubil. Dacă H_{s-3}/H_{s-2} este rezolubil, rezultă din teorema 1.3 că și H_{s-3} este rezolubil. Recursiv, obținem în final că $H_0 = G$ este rezolubil.

Corolarul 4.3. *Fie E o extindere normală și radicală a corpului K. Dacă F este o extindere normală a lui K astfel încît $K \subseteq F \subseteq E$, atunci $G(F/K)$ este rezolubil.*

Demonstrație. Avem

$$G(F/K) \simeq \frac{G(E/K)}{G(E/F)}.$$

Din teorema 4.2 și teorema 1.3 obținem că $G(F/K)$ este grup rezolubil.

Teorema 4.4. *Fie K un corp și E o extindere normală a corpului K astfel încît $G(E/K)$ este rezolubil. Atunci există o extindere F a lui K ce conține pe E, astfel încît F este o extindere normală și radicală a corpului K.*

Demonstrație. Punem $G = G(E/K)$. Deoarece G este rezolubil, există un șir normal

$$G = H_0 \supset H_1 \supset \dots \supset H_s = \{e\}$$

astfel încît H_{i-1}/H_i este abelian $(1 \leqslant i \leqslant s)$. Dacă G este un grup finit, atunci H_{i-1}/H_i sînt grupuri finite și abeliene. Deci putem presupune că H_{i-1}/H_i $(1 \leqslant i \leqslant s)$ sînt ciclice.

Vom proceda prin inducție după s. Dacă $s = 1$, atunci $G = H_0 \supset H_1 = \{e\}$ și deci G este ciclic. Fie $n = \text{ord}\, G$. Considerăm ξ o rădăcină primitivă a unității de ordinul n. Notăm $F = K(\xi)E$ și fie $H = G(F/K(\xi))$. Funcția $\varphi : H \to G$, $\varphi(\sigma) = \sigma | E$ este un omomorfism injectiv de grupuri.

Deoarece G este ciclic, avem că H este ciclic. Dacă $m = \text{ord}\, H$, atunci din teorema lui Lagrange rezultă că $m | n$.

Fie η o rădăcină primitivă a unității, de ordinul m. Cum $\eta^m = 1$, atunci $\eta^n = 1$ și deci există $a \in \mathbb{Z}$ așa încît $\eta = \xi^a$. Deci $\eta \in K(\xi)$. Din teorema 3.3 rezultă că F este o extindere radicală simplă a lui $K(\xi)$. Cum $K(\xi)$ este o extindere radicală simplă a lui K, rezultă că F este o extindere radicală a lui K. Dar $F = K(\xi)E$ și $K(\xi)$ și E fiind extinderi normale ale lui K, atunci F este o extindere normală a lui K. Presupunem afirmația adevărată pentru $s - 1$ și o demonstrăm pentru s. Să punem $E_1 = E^{H_1} = \{\alpha \in E | \sigma(\alpha) = \alpha$, oricare ar fi $\sigma \in H_1\}$. Din teorema fundamentală a lui Galois, $G(E/E_1) \simeq H_1$, și H_1 fiind subgrup normal în G, atunci E_1 este normală peste K și $G(E_1/K) \simeq G/H_1$. Deci $G(E_1/K)$ este ciclic. Astfel, există o extindere radicală și normală F_1 a lui K ce conține pe E_1. Atunci EF_1 este o extindere normală a lui K și $G(EF_1/F_1)$ este izomorf cu un subgrup al lui $G(E/E_1) = H_1$. Conform ipotezei de inducție [deoarece H_1 are un șir normal de lungime $s - 1$, atunci $G(EF_2/F_1)$ are un șir normal de lungime $s - 1$] există o extindere F_2 a lui F_1 care este normală și radicală. F_1 fiind extindere radicală a lui K, atunci F_2 este extindere radicală a lui K. Din teorema 4.1 există o extindere radicală și normală L a lui K ce conține pe F_2.

Definiția 4.1. Fie E o extindere finită a lui K. Se spune că E este *rezolvabilă prin radicali* dacă există o extindere radicală F a lui K astfel încît $E \subseteq F$.

Definiția 4.2. Extinderea finită E a lui K se numește *rezolubilă* dacă există o extindere normală F a lui K astfel încît $G(F/K)$ este un grup rezolubil.

Propoziția 4.5. *Definiția* 4.1 *este echivalentă cu definiția* 4.2.

Demonstrație. Fie F o extindere radicală a lui K ce conține pe E. Ținînd seama de teorema 4.1, putem presupune că F este și normală. Atunci $G(F/K)$ este rezolubil (teorema 4.2). Deci dacă E este rezolvabilă prin radicali, atunci E este rezolubilă.

Reciproc, presupunem că E este rezolubilă. Atunci există o extindere normală F a lui K astfel încît $G(F/K)$ este grup rezolubil. Din teorema 4.4 rezultă că există o extindere F' a lui K normală și radicală ce conține pe F. Deci E este o extindere rezolvabilă prin radicali.

§ 5. Rezolvarea ecuațiilor algebrice prin radicali

Definiția 5.1. Fie K un corp. Se spune că un număr complex α *se exprimă prin radicali* (*relativ la* K) dacă extinderea $K(\alpha)$ a lui K este rezolvabilă prin radicali (sau, echivalent, există o extindere radicală E a lui K astfel încît $\alpha \in E$). Dacă numărul complex α se exprimă prin radicali relativ la corpul $\mathbb{Q}$, atunci spunem simplu că α *se exprimă prin radicali.* Dacă $\alpha_1, \alpha_2, \ldots, \alpha_n$ sînt numere complexe și α este un număr complex care se exprimă prin radicali relativ la corpul $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, spunem că α se exprimă prin radicali relativ la numerele complexe $\alpha_1, \alpha_2, \ldots, \alpha_n$. Este ușor de văzut că această noțiune este aceeași cu cea dată în cap. IV, § 1.

Definiția 5.2. Fie $f \in K[X]$, grad $f \geqslant 1$. Ecuația $f = 0$ se numește *rezolvabilă prin radicali* dacă toate rădăcinile sale se exprimă prin radicali relativ la K.

Propoziția 5.1. *Fie $f \in K[X]$ un polinom ireductibil. Atunci ecuația $f = 0$ este rezolvabilă prin radicali, dacă cel puțin o rădăcină a sa se exprimă prin radicali relativ la corpul K.*

Demonstrație. Fie α o rădăcină a lui f ce se exprimă prin radicali. Deci, există o extindere normală și radicală E a lui K ce conține pe α. Deoarece f este ireductibil, rezultă că toate rădăcinile lui f aparțin lui E. Deci ecuația $f = 0$ este rezolvabilă prin radicali.

Propoziția 5.2. *Fie K un corp. Mulțimea numerelor complexe ce se exprimă prin radicali relativ la K formează un subcorp al lui $\mathbb{C}$.*

Demonstrație. Fie α, β două numere complexe ce se exprimă prin radicali. Există extinderile radicale E și F ale lui K astfel încît $\alpha \in E$ și $\beta \in F$. Pentru E există șirul de extinderi

$$K = E_0 \subset E_1 \subset \ldots \subset E_s = E,$$

unde E_i este o extindere radicală simplă a lui E_{i-1} $(1 \leqslant i \leqslant s)$. Pentru F există șirul de extinderi

$$K = F_0 \subset F_1 \subset \ldots \subset F_r = F$$

astfel încît F_j este o extindere radicală simplă a lui F_{j-1} $(1 \leqslant j \leqslant r)$. Luăm compozitul EF. Avem șirul de extinderi

$$K \subset E_0 \subset E_1 \subset \ldots \subset E_s = E \subset EF_1 \subset EF_2 \subset \ldots$$

$$\ldots \subset EF_r = EF.$$

Se vede ușor că EF_j este radicală simplă peste EF_{j-1} $(1 \leqslant j \leqslant r)$. Atunci rezultă că EF este o extindere radicală a lui K. Deoarece $\alpha + \beta$, $\alpha\beta \in EF$ și dacă $\alpha \neq 0$, atunci $\alpha^{-1} \in EF$; rezultă că mulțimea numerelor complexe ce se exprimă prin radicali relativ la K este un subcorp al lui $\mathbb{C}$.

Teorema 5.3. (*Criteriu de rezolvabilitate al unei ecuații prin radicali*). *Fie K un corp și $f \in K[X]$ un polinom ireductibil. Ecuația $f = 0$ este rezolvabilă prin radicali dacă și numai dacă grupul Galois al polinomului f este rezolubil.*

Demonstrație. Fie E corpul de descompunere al polinomului f și $G = G(E/K)$ grupul Galois asociat. Dacă ecuația $f = 0$ este rezolvabilă prin radicali, există o extindere normală și radicală F a lui K ce conține rădăcinile $\alpha_1, \alpha_2, \ldots, \alpha_n$ ale polinomului f. Întrucît $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset F$, avem

$$G(E/K) \simeq \frac{G(F/K)}{G(F/E)}$$

și deci $G(E/K)$ este rezolubil. Reciproc, presupunem că $G = G(E/K)$ este rezolubil. Atunci, din teorema 4.4, există o

extindere F a lui K, normală şi radicală, ce conţine pe E. Deci $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ şi prin urmare ecuaţia $f = 0$ este rezolvabilă prin radicali.

Corolarul 5.4. *Fie K un corp şi $f \in K[X]$ un polinom cu grad $(f) \leqslant 4$. Atunci ecuaţia $f = 0$ este rezolvabilă prin radicali.*

Demonstraţie. Putem presupune că f este ireductibil. Fie G_f grupul Galois al polinomului f. Din propoziţia 11.1 rezultă că G_f este izomorf cu un subgrup al grupului σ_n, unde $n = \text{grad}(f)$. Dar σ_n fiind rezolubil pentru $n \leqslant 4$, corolarul 5.4 rezultă din teorema 5.3.

Observaţii. **1.** Din teorema 11.4, cap. VI, pentru orice număr prim $p \geqslant 5$ există un polinom $f(X)$ de grad p avînd grupul Galois asociat izomorf cu σ_p. Cum σ_p nu este rezolubil, rezultă că ecuaţia $f(X) = 0$ nu este rezolvabilă prin radicali (relativ la corpul $\mathbb{Q}$).

2. Fie $f \in \mathbb{R}[X]$ un polinom arbitrar. Ecuaţia $f = 0$ este rezolvabilă prin radicali relativ la corpul $\mathbb{R}$. Într-adevăr, f se descompune într-un produs finit de polinoame de gradul $\leqslant 2$ cu coeficienţi în $\mathbb{R}$. Atunci putem presupune $f \in \mathbb{R}[X]$ cu grad $f \leqslant 2$. Dar ecuaţia $f = 0$ este rezolvabilă prin radicali relativ la corpul $\mathbb{R}$. Greutatea însă constă în faptul de a scrie un polinom $f \in \mathbb{R}[X]$ ca un produs finit de polinoame ireductibile de grad $\leqslant 2$.

§ 6. Cîteva observaţii asupra corpurilor de caracteristică zero

Pînă în prezent, corpurile care au intervenit au fost subcorpuri ale corpului numerelor complexe. Este uşor de văzut că întreaga teorie expusă în capitolele VI şi VII pînă la acest paragraf rămîne valabilă, fără nici un fel de modificări, pentru corpurile de caracteristică zero. Un corp K are caracteristica zero dacă $n \cdot 1 \neq 0$ pentru orice număr întreg $n \neq 0$ ($1 \in K$ fiind unitatea corpului). Un exemplu de corp de caracteristică zero care nu este corp de numere complexe se obţine în felul următor. Fie K un corp (de numere complexe) şi $X_1, X_2, \ldots, X_n$, nedeterminate. Corpul $E = k(X_1, \ldots, X_n)$ al fracţiilor raţionale este un corp de caracteristică zero. Singura noţiune care trebuie explicată mai mult este cea de corp de descompunere al unui polinom cu coeficienţi într-un corp de caracteristică zero. Mai precis, apare problema unicităţii corpului de descompunere al unui polinom. Fiind dat un corp arbitrar K şi $f \in K[X]$, un polinom cu $n = \text{grad}(f) \geqslant 1$ se numeşte *corp de descompunere* al lui

f o extindere, E a lui K astfel încît f se descompune în factorii liniari în E și $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ unde $\alpha_1, \alpha_2, \ldots, \alpha_n$ sînt rădăcinile lui f.

Propoziția 6.1. *Fie K un corp și $f \in K[X]$ cu $n = grad\, f \geqslant 1$. Atunci există un corp de descompunere al polinomului f.*

Demonstrație. Din propoziția 4.5, cap. III, există o extindere F a lui K astfel încît f are n rădăcini $\alpha_1, \alpha_2, \ldots, \alpha_n$ în F. Este clar că un corp de descompunere a lui f este $E = K(\alpha_1, \ldots, \alpha_n)$.

Propoziția 6.2. *Fie K și K' două corpuri și $\sigma : K \to K'$ un izomorfism de corpuri. Fie $f = a_0 + a_1X + \ldots + a_nX^n$ un polinom din $K[X]$ cu $n = grad f \geqslant 1$. Vom nota cu f^σ polinomul $f^\sigma = \sigma(a_0) + \sigma(a_1)X + \ldots + \sigma(a_n)X^n \in K'[X]$. Dacă E este un corp de descompunere al lui f și E' este un corp de descompunere a lui f^σ, există un izomorfism $\tau : E \to E'$ astfel încît $\tau|K = \sigma$.*

Demonstrație. Fie $\alpha_1, \alpha_2, \ldots, \alpha_n$ rădăcinile lui f în E iar $\beta_1, \beta_2, \ldots, \beta_n$ rădăcinile lui f^σ în E'. Atunci $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ și $E' = K'(\beta_1, \beta_2, \ldots, \beta_n)$.

Fie f_1 polinomul minimal al lui α_1 peste K. Rezultă $f_1|f$ și deci $f_1^\sigma|f^\sigma$. Polinomul f_1 fiind ireductibil, rezultă că și f_1^σ este ireductibil în $K'[X]$. Rădăcinile lui f_1^σ se găsesc printre rădăcinile lui f^σ. Putem presupune că β_1 este rădăcină a lui f_1^σ. Notăm cu $E_1 = K(\alpha_1)$ și $E_1' = K'(\beta_1)$. Fie $x \in K(\alpha_1)$ un element arbitrar. Există un polinom $g \in K[X]$ astfel încît $x = g(\alpha_1)$. Definim aplicația

$$\tau_1 : E_1 \to E_1',$$

$$\tau_1(x) = g^\sigma(\beta_1).$$

Dacă $x = g(\alpha_1) = g'(\alpha_1)$, atunci $(g-g')(\alpha_1) = 0$ și deci $f_1|(g-g')$. Rezultă că $f_1^\sigma|g^\sigma - g'^\sigma$ și deci $(g^\sigma - g'^\sigma)(\beta_1) = 0$, adică $g^\sigma(\beta_1) = g'^\sigma(\beta_1)$ și aplicația τ_1 este bine definită. Se vede ușor că τ_1 este omomorfism de corpuri și $\tau_1|K = \sigma$. Din definiția lui τ_1 se vede că este o aplicație bijectivă. Să notăm cu $E_i = K(\alpha_1, \ldots, \alpha_i)$ și fie $E_i' = K'(\beta_1, \ldots, \beta_i)$ și să presupunem că am construit izomorfismul $\tau_i : E_i \to E_i'$ astfel încît $\tau_i|K = \sigma$. Luăm α_{i+1} și fie f_{i+1} polinomul său minimal peste E_i. Cum $f_{i+1}(\alpha_{i+1}) = 0$, rezultă că $f_{i+1}|f$ și deci $f_{i+1}^{\tau_i}|f^{\tau_i}$. Dar $f^{\tau_i} = f^\sigma$. Rezultă că rădăcinile lui $f_{i+1}^{\tau_i}$ se găsesc printre rădăcinile lui f^σ. Presupu-

nem că β_{i+1} este o rădăcină a lui $f_{i+1}^{\tau i}$. Cum $f_{i+1}^{\tau i}$ este ireductibil, atunci $f_{i+1}^{\tau i}$ este polinomul minimal al lui β_{i+1} peste corpul E_i'. Exact ca la pasul $i = 1$, există un izomorfism $\tau_{i+1} : E_{i+1} \to E_{i+1}'$ astfel încît $\tau_{i+1}|E_i = \tau_i$. Deci, există un izomorfism $\tau : E \to E'$ astfel încît $\tau|K = \sigma$.

Corolarul 6.3. *Fie K un corp și $f \in K[X]$ un polinom cu* grad $(f) \geqslant 1$. *Atunci corpul de descompunere al polinomului f este unic determinat pînă la un izomorfism.*

§ 7. Teorema Abel-Ruffini

Fie K un corp (de numere complexe) și $X_1, X_2, \ldots, X_n$ n nedeterminate. Corpul $E = K(X_1, X_2, \ldots, X_n)$ al fracțiilor raționale este un corp de caracteristică zero.

Fie $\boldsymbol{\sigma}_n$ grupul permutărilor de n elemente. Pentru fiecare $\sigma \in \boldsymbol{\sigma}_n$ există K-automorfismul

$$\sigma^* : E \to E$$

astfel încît $\sigma^*(X_i) = X_{\sigma(i)}$ $(1 \leqslant i \leqslant n)$. Mulțimea $G = \{\sigma^* | \sigma \in \boldsymbol{\sigma}_n\}$ este un grup de K-automorfisme izomorf cu $\boldsymbol{\sigma}_n$. Ținînd seama de propoziția 6.7, cap. III, $F = E^G = K(s_1, s_2, \ldots, s_n)$, unde $s_1, s_2, \ldots, s_n$ sînt polinoamele simetrice fundamentale. Din lema 9.1, cap. VI, rezultă $G(E/F) = G \simeq \boldsymbol{\sigma}_n$. Fie polinomul $f(X) = (X - X_1)(X - X_2) \ldots (X - X_n) \in K(X_1, \ldots, X_n)[X]$. Se vede ușor că $f(X) \in K(s_1, s_2, \ldots, s_n)[X] = F[X]$ și corpul de descompunere al lui $f(X)$ peste F este E, deci E este o extindere normală a lui F. Polinomul $f(X)$ este ireductibil în inelul $F[X]$. Într-adevăr, dacă $f = gh$ cu grad $g \geqslant 1$ și grad $h \geqslant 1$, atunci $g = (X - X_{i_1}) \ldots (X - X_{i_k})$, $1 \leqslant k \leqslant n$, de unde rezultă că $(-1)^k X_{i_1} \ldots X_{i_k} \in K(s_1, \ldots, s_n)$, adică $X_{i_1} \ldots X_{i_k}$ este polinom simetric, ceea ce este o contradicție.

Fie K un corp de numere și $t_1, \ldots, t_n$, nedeterminate distincte. Considerăm polinomul $f(X) = X^n - t_1 X^{n-1} + t_2 X^{n-2} + \ldots + (-1)^n t_n \in K(t_1, t_2, \ldots, t_n)[X]$. Ecuația $f(X) = 0$ se numește *ecuația generală de gradul n* peste corpul K.

Fie E corpul de descompunere al polinomului $f(X)$ peste corpul $F = K(t_1, t_2, \ldots, t_n)$. Dacă $y_1, y_2, \ldots, y_n$ sînt rădăcinile polinomului $f(X)$, atunci $E = F(y_1, y_2, \ldots, y_n)$. Cum $f(X) = (X - y_1)(X - y_2) \ldots (X - y_n)$, egalitățile

$$t_1 = y_1 + y_2 + \ldots + y_n = \sum_{i=1}^{n} y_i,\ t_2 = \sum_{1 \leqslant i < j \leqslant n} y_i y_j, \ldots, t_n = y_1 y_2 \ldots y_n.$$

Deci se obține

$$E = F(y_1, y_2, \ldots, y_n) = K(t_1, t_2, \ldots, t_n)(y_1, y_2, \ldots, y_n) =$$

$$= K(t_1, t_2, \ldots, t_n, y_1, \ldots, y_n) = K(y_1, y_2, \ldots, y_n).$$

Fie $X_1, X_2, \ldots, X_n$ nedeterminate distincte și $s_1, s_2, \ldots, s_n$ polinoamele simetrice fundamentale. Avem extinderile

$$K(t_1, t_2, \ldots, t_n) \subset K(y_1, y_2, \ldots, y_n),$$

$$K(s_1, s_2, \ldots, s_n) \subset K(X_1, X_2, \ldots, X_n).$$

Considerăm aplicația de inele

$$\sigma : K[t_1, t_2, \ldots, t_n] \to K(s_1, s_2, \ldots, s_n),$$

$$\sigma(t_i) = s_i \quad (1 \leqslant i \leqslant n).$$

Această aplicație se extinde la un K-omomorfism de corpuri

$$\tau : K(t_1, t_2, \ldots, t_n) \to K(s_1, s_2, \ldots, s_n),$$

$$\tau(t_i) = s_i \quad (1 \leqslant i \leqslant n).$$

τ se definește astfel :

$$\tau\left(\frac{P(t_1, \ldots, t_n)}{Q(t_1, \ldots, t_n)}\right) = \frac{P(s_1, s_2, \ldots, s_n)}{Q(s_1, s_2, \ldots, s_n)}.$$

Analog, există un K-omomorfism de corpuri

$$\theta : K(X_1, \ldots, X_n) \to K(y_1, \ldots, y_n),$$

$$\theta\left(\frac{P(X_1, \ldots, X_n)}{Q(X_1, \ldots, X_n)}\right) = \frac{P(y_1, \ldots, y_n)}{Q(y_1, \ldots, y_n)}.$$

$\tau : K(t_1, t_2, \ldots, t_n) \to K(s_1, s_2, \ldots, s_n)$ este injectivă. Într-adevăr, dacă

$$z = \frac{P(t_1, \ldots, t_n)}{Q(t_1, \ldots, t_n)} \in K(t_1, t_2, \ldots, t_n),$$

atunci

$$\tau(z) = \frac{P(s_1, \ldots, s_n)}{Q(s_1, \ldots, s_n)}, \text{ de unde } \theta\tau(z) = \frac{P(\theta(s_1), \ldots, \theta(s_n))}{Q(\theta(s_1), \ldots, \theta(s_n))}.$$

Deoarece $s_1 = \sum_{i=1}^{n} X_i$, $s_2 = \sum_{i<j} X_i X_j, \ldots, s_n = X_1 \ldots X_n$, atunci $\theta(s_1) = t_1$, $\theta(s_2) = t_2, \ldots, \theta(s_n) = t_n$ şi deci $\theta(\tau(z)) = \frac{P(t_1, \ldots, t_n)}{Q(t_1, \ldots, t_n)} = z$. Din egalitatea $\theta(\tau(z)) = z$ rezultă imediat că τ este injectivă. Dar se vede uşor că τ este surjectivă şi deci τ este un K-izomorfism. Polinomului

$$f(X) = X^n - t_1 X^{n-1} + \ldots + (-1)^n t_n \in K(t_1, \ldots, t_n)[X]$$

îi asociem polinomul

$$f^{\tau}(X) = X^n - \tau(t_1) X^{n-1} + \ldots + (-1)^n \tau(t_n) \in K(s_1, \ldots, s_n)[X]$$

sau $f^{\tau}(X) = X^n - s_1 X^{n-1} + \ldots + (-1)^n s_n = (X - X_1)(X - X_2) \ldots (X - X_n)$. Cum corpul de descompunere al lui $f(X)$ este $K(y_1, \ldots, y_n)$ şi corpul de descompunere al lui $f^{\tau}(X)$ este $K(X_1, \ldots, X_n)$, există un K-izomorfism $\alpha : K(y_1, \ldots, y_n) \to K(X_1, \ldots, X_n)$ astfel încît $\alpha | K(t_1, \ldots, t_n) = \tau$ (vezi propoziţia 6.2). Rezultă atunci că

$$G(K(y_1, \ldots, y_n)/K(t_1, \ldots, t_n)) \simeq G(K(X_1, \ldots, X_n)/K(s_1, \ldots, s_n)) \simeq \sigma_n$$

Dar după cum s-a văzut, $f\tau(X)$ fiind ireductibil, rezultă că polinomul $f(X)$ este ireductibil. Într-adevăr, dacă $f = gh$ cu grad $g \geqslant 1$ şi grad $h \geqslant 1$, atunci $f^{\tau}(X) = g^{\tau}(X) \cdot h^{\tau}(X)$, adică se obţine o contradicţie.

Ţinînd seama de cele demonstrate mai înainte, rezultă

Teorema 7.1. *Fie polinomul*

$$f(X) = X^n - t_1 X^{n-1} + \ldots + (-1)^n t_n \in K(t_1, \ldots t_n)[X].$$

1) *Grupul Galois al polinomului f este izomorf cu σ_n.*
2) *f este ireductibil.*

Teorema 7.2 (*Abel-Ruffini*). *Ecuaţia generală $f(x) = 0$ nu este rezolvabilă prin radicali pentru $n \geqslant 5$.* (*Pentru $n \leqslant 4$, ecuaţia generală este rezolvabilă prin radicali*).

VIII

CONSTRUCȚII CU RIGLA ȘI COMPASUL

§ 1. Problema geometrică și transpunerea ei algebrică

Fie ω un plan și $S = \{P_1, \ldots, P_n\}$ o mulțime finită de puncte din planul ω. Recursiv, se definesc mulțimile de puncte $S_1, S_2, \ldots$ $\ldots, S_n, \ldots$ Punem $S_1 = S$ și presupunem definită mulțimea S_r. Atunci S_{r+1} este egală cu S_r la care se adaugă punctele care se obțin prin următoarele trei reguli:

1. Punctele ce sînt intersecții de drepte determinate de perechi de puncte din S_r.

2. Punctele ce se obțin prin intersecția unei drepte determinate din două puncte din S_r cu un cerc care are centrul în S_r și raza egală cu un segment determinat de două puncte din S_r.

3. Punctele ce se obțin prin intersecția a două cercuri cu centrele în S_r și razele egale cu segmente determinate de perechi de puncte din S_r.

În felul acesta se obține șirul crescător de mulțimi finite: $S_1 \subseteq S_2 \subseteq \ldots \subseteq S_r \subseteq \ldots$

Notăm $C(P_1, P_2, P_3, \ldots, P_n) = \bigcup_{r \geqslant 1} S_r$. Un punct P ce aparține mulțimii $C(P_1, P_2, \ldots, P_n)$ se spune că se obține prin construcția cu rigla și compasul din punctele $P_1, P_2, \ldots, P_n$. Se observă că dacă $S = \{P_1\}$, atunci $C(P_1) = \{P_1\}$. Se pune în mod natural întrebarea dacă acest punct de vedere corespunde cu cel din geometria euclidiană. Elementele care sînt date, respectiv care se cer determinate într-o construcție cu rigla și compasul din geometria euclidiană, pot fi puncte, drepte,

cercuri, unghiuri într-un număr finit fiecare. Elementelor date li se poate asocia o mulțime finită de puncte : o dreaptă este determinată de două puncte, un cerc este determinat de centrul său și un punct de pe frontiera sa, unghiul este determinat de trei puncte și anume vîrful său și două puncte egal depărtate de vîrf.

Să vedem cum se transpune algebric problema geometrică de construcție cu rigla și compasul. Pentru aceasta, considerăm

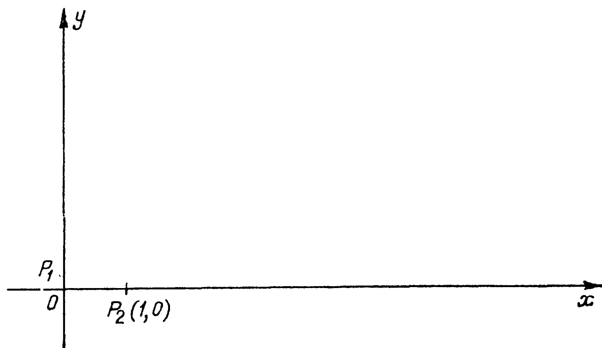


Fig. 12

în planul ω un sistem de axe xOy, cu originea în punctul P_1, iar P_2 să fie de coordonate (1, 0), adică P_1P_2 să fie unitatea de măsură. Considerăm aplicația $\theta : \omega \rightarrow \mathbb{C}$, $\theta(P) = x + iy$, unde P este de coordonate (x, y), unde θ este o aplicație bijectivă, numărul complex $x + iy$ avînd punctul $P(x, y)$ ca afix. Să notăm $\theta(P_i) = \alpha_i$ $(1 \leqslant i \leqslant n)$. Deci $\alpha_1 = 0$ și $\alpha_2 = 1$. Notăm $\theta(C(P_1, P_2, \ldots, P_n)) = C(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Un număr complex α ce aparține mulțimii $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ se obține *prin construcția cu rigla și compasul* din numerele complexe $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Teorema 1.1. *$C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ este subcorp al lui $\mathbb{C}$ avînd proprietățile următoare :*

1) *este închis la conjugare, adică dacă $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, atunci și $\bar{\alpha} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$;*

2) *este închis la extragerea rădăcinii pătrate, adică dacă $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, atunci și $\sqrt{\alpha} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$.*

În plus, $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ este cel mai mic subcorp al lui $\mathbb{C}$ ce conține numerele complexe $\alpha_1, \alpha_2, \ldots, \alpha_n$ și are proprietățile 1 *și* 2.

Demonstrație. Fie α, $\alpha' \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Să notăm cu P și P' punctele din ω astfel încît $\theta(P) = \alpha$ și $\theta(P') = \alpha'$. Deci P, $P' \in C(P_1, P_2, \ldots, P_n)$.

Punctul Q obținut prin regula paralelogramului (fig. 13) corespunde numărului complex $\alpha + \alpha'$. Dar se vede ușor că

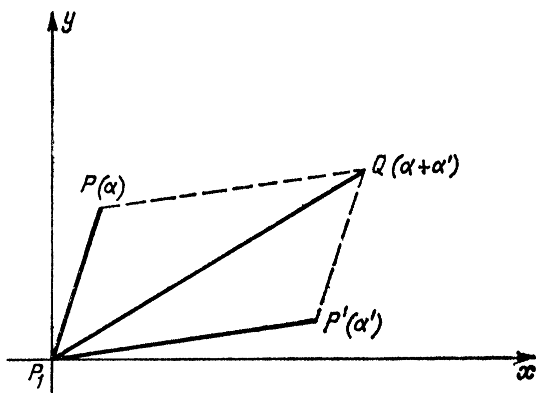


Fig. 13

Q se poate construi cu rigla și compasul, adică $Q \in C(P_1, \ldots, P_n)$ și deci $\alpha + \alpha' \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Scriem pe α și α' sub formă trigonometrică:

$$\alpha = r(\cos \varphi + i \sin \varphi),$$

$$\alpha' = r' (\cos \varphi + i \sin \varphi);$$

atunci $\alpha\alpha' = rr' [\cos (\varphi + \varphi') + i \sin (\varphi + \varphi')]$. Deoarece $\varphi + \varphi'$ se construiește ușor cu rigla și compasul, să construim și produsul rr' cu rigla și compasul. Din asemănarea triunghiurilor dreptunghice (fig. 14) avem

$$\frac{x}{r} = \frac{r'}{1}, \text{ de unde } x = rr'.$$

Se vede din fig. 14, că punctul X se poate construi cu rigla și compasul. Deci $\alpha\alpha' \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Dacă $\alpha \in C(\alpha_1, \alpha_2, \ldots \ldots, \alpha_n)$, $\alpha \neq 0$, atunci $\alpha^{-1} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Într-adevăr, dacă

$$\alpha = r (\cos \varphi + i \sin \varphi),$$

atunci

$$\alpha^{-1} = \frac{1}{r}\,[\cos(-\varphi) + i \sin(-\varphi)\,.$$

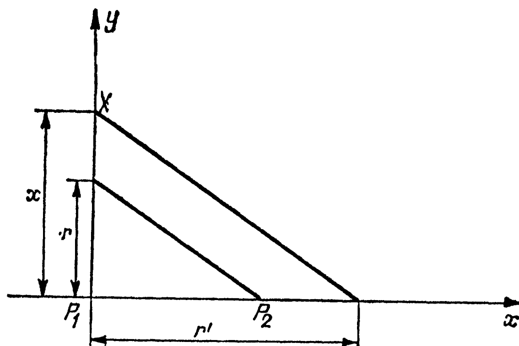


Fig. 14

Din fig. 15 reiese că

$$\frac{x}{1} = \frac{1}{r} \text{ şi deci } x = \frac{1}{r}.$$

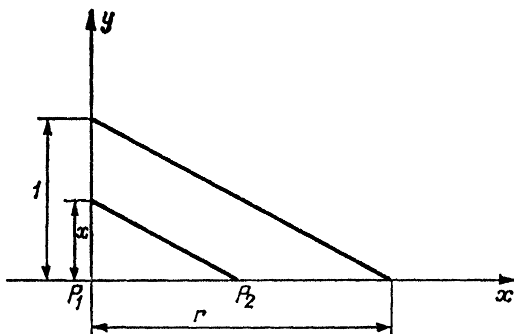


Fig. 15

Deoarece x se poate construi cu rigla şi compasul, rezultă că $\alpha^{-1} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Deci $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ este un subcorp al lui $\mathbb{C}$.

a) Fie $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Din fig. 16 se vede uşor că şi $\bar{\alpha} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

b) Fie $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Dacă scriem $\alpha = r(\cos\varphi + i\sin\varphi)$, atunci $\sqrt{\alpha} = \sqrt{r}\left(\cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2}\right)$. Din fig. 17, din triunghiul dreptunghic AP_1B avem egalitatea

$$x^2 = P_1P_2 \cdot P_2A = 1 \cdot r, \text{ de unde } x = \sqrt{r}.$$

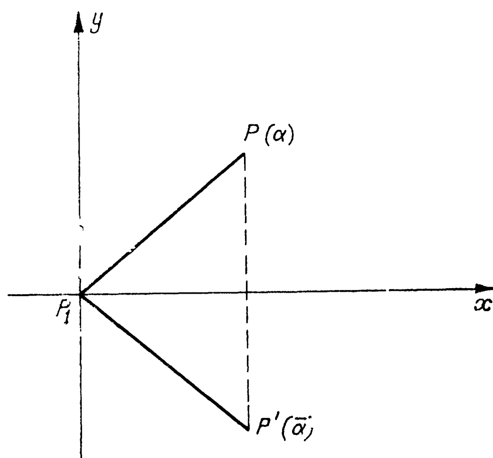


Fig. 16

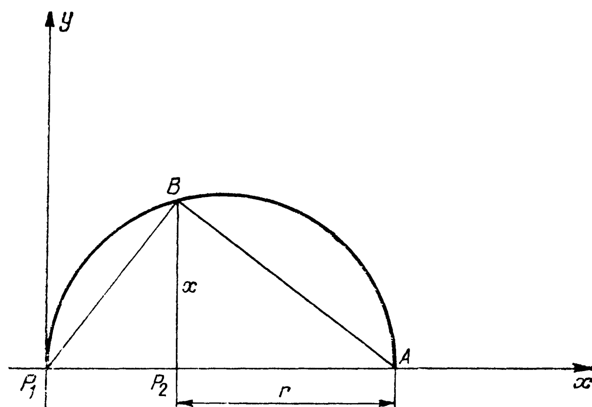


Fig. 17

Deoarece $\sqrt{r}$ şi $\frac{\varphi}{2}$ se pot construi cu rigla şi compasul, rezultă că $\sqrt{\alpha} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Fie K un subcorp al lui $\mathbb{C}$ ce conţine pe $\alpha_1, \alpha_2, \ldots, \alpha_n$ şi are proprietăţile 1 şi 2. Cum $-1 \in K$, din proprietatea 1 rezultă că $\mathrm{i} = \sqrt{-1} \in K$. Dacă $\alpha = x + \mathrm{i}y \in K$, atunci tot din a) avem $\overline{\alpha} = x - \mathrm{i}y \in K$, de unde rezultă că $x, y \in K$. Deci

$$\alpha = x + \mathrm{i}y \in K \Leftrightarrow x, y \in K.$$

Prin aplicaţia $\theta : \omega \to \mathbb{C}$ să notăm $\omega' = \theta^{-1}(K)$. Să arătăm că ω' are următoarele trei proprietăţi :

1°. Intersecţia a două drepte determinate de puncte ce aparţin lui ω' aparţine lui ω'.

2°. Intersecţia unei drepte determinate de două puncte din ω' cu un cerc de centru un punct din ω' iar raza egală cu un segment determinat de două puncte din ω' aparţine lui ω'.

3°. Intersecţia a două cercuri de centre puncte din ω' şi raze egale cu segmente determinate de puncte din ω' aparţine lui ω'.

Să verificăm 1°. Aceasta rezultă din faptul că soluţia sistemului de ecuaţii

$$\begin{cases} ax + by + c = 0, & a, b, c, a', b', c' \in K, \\ a'x + b'y + c' = 0, \end{cases}$$

este formată din elemente din K. Afirmaţia 2° rezultă din faptul că soluţia sistemului

$$\begin{cases} ax + by + c = 0, & a, b, c, m, n, p \in K, \\ x^2 + y^2 + mx + ny + p = 0, \end{cases}$$

este formată din elemente din K (corpul K avînd proprietatea b) din teorema 8.1).

Afirmaţia 3° rezultă din 2°, deoarece intersecţia a două cercuri revine la intersecţia unuia dintre cercuri cu axa radicală a cercurilor. Cum $P_1, P_2, \ldots, P_n \in \omega'$, atunci din 1°, 2° şi 3° rezultă că $C(P_1, P_2, \ldots, P_n) \subseteq \omega'$ şi deci $C(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq K$, ceea ce înseamnă că $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ este cel mai mic subcorp al lui $\mathbb{C}$ ce conţine numerele $\alpha_1, \alpha_2, \ldots, \alpha_n$ şi are proprietăţile 1 şi 2.

§ 2. Primul criteriu de constructibilitate cu rigla și compasul

Considerăm mulțimea de puncte $S = \{P_1, \ldots, P_n\}$ din planul ω, $C(P_1, P_2, \ldots, P_n)$ mulțimea de puncte constructibile cu rigla și compasul iar $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ subcorpul lui $\mathbb{C}$ asociat mulțimii $C(P_1, P_2, \ldots, P_n)$. Deoarece $\mathbb{Q} \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, avem $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n) \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Vom nota $F = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n)$.

Teorema 2.1 (*primul criteriu de constructibilitate cu rigla și compasul*). *Numărul complex α este constructibil cu rigla și compasul din numerele $\alpha_1, \alpha_2, \ldots, \alpha_n$ dacă și numai dacă există un lanț ascendent finit de extinderi*

$$F = F_0 \subset F_1 \subset \ldots \subset F_r$$

astfel încît $\alpha \in F_r$ și $[F_i : F_{i-1}] \leqslant 2$ pentru orice $1 \leqslant i \leqslant r$.

Demonstrație. Notăm cu $K = \{\alpha \in \mathbb{C} \mid$ există șirul de extinderi $F = F_0 \subset F_1 \subset \ldots \subset F_r$ astfel încît $\alpha \in F_r$ și $[F_i : F_{i-1}] \leqslant 2$, oricare ar fi $1 \leqslant i \leqslant r\}$.

Fie $\alpha, \beta \in K$; există șirurile finite de extinderi $F = F_0 \subset F_1 \subset \ldots \subset F_r$, unde $\alpha \in F_r$ și $[F_i : F_{i-1}] \leqslant 2$, $1 \leqslant i \leqslant r$, și $F = F'_0 \subset F'_1 \subset \ldots \subset F'_{r'}$, unde $\beta \in F'_{r'}$ și $[F'_j : F'_{j-1}] \leqslant 2$, $1 \leqslant j \leqslant r'$. Se obține șirul de extinderi

$$F = F_0 \subset F_1 \subset \ldots \subset F_r = F_rF'_0 \subset F_rF'_1 \subset \ldots \subset F_rF'_{r'},$$

unde $[F_rF'_j : F_rF'_{j-1}] \leqslant 2$, oricare ar fi $1 \leqslant j \leqslant r'$. Cum $\alpha + \beta$, $\alpha\beta \in F_rF'_{r'}$ și $\alpha^{-1} \in F_r$, dacă $\alpha \neq 0$, rezultă că K este un subcorp al lui $\mathbb{C}$. Cum F este închis la operația de conjugare, rezultă că și corpul K este închis la operația de conjugare. Dacă $F = F_0 \subset F_1 \subset \ldots \subset F_r$ este un șir de extinderi astfel încît $[F_i : F_{i-1}] \leqslant 2$, $1 \leqslant i \leqslant r$, atunci fiecare F_i este închis la extragerea rădăcinii pătrate. Deci K este închis la extragerea rădăcinii pătrate. Întrucît $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$, din teorema 1.1 rezultă că $C(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq K$. Fie $\alpha \in K$ și fie șirul de extinderi

$$F = F_0 \subset F_1 \subset \ldots \subset F_r$$

astfel încît $\alpha \in F_r$ și $[F_i : F_{i-1}] \leqslant 2$, oricare ar fi $1 \leqslant i \leqslant r$. Verificăm prin inducție că pentru orice i, $F_i \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Pentru $i = 0$, $F_0 = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \ldots, \bar{\alpha}_n) \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Să presupunem că $F_i \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ și să arătăm că și $F_{i+1} \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Deoarece $[F_{i+1} : F_i] \leqslant 2$, avem $F_{i+1} = F_i(\beta)$, unde β este un element algebric peste F_i al cărui polinom minimal f este de grad $\leqslant 2$. Deci β este rădăcina unei ecuații de gradul doi cu coeficienți în $F_i \subseteq C(\alpha_1, \ldots, \alpha_n)$. Dar $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ are proprietatea 2, rezultă că $\beta \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ și deci $F_{i+1} \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Deci, am arătat că și $K \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, de unde rezultă egalitatea $K = C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ și deci teorema 2.1.

Corolarul 2.2. *Dacă $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, atunci polinomul minimal al lui α peste corpul $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \ldots, \bar{\alpha}_n)$ este de grad egal cu o putere a lui 2.*

Demonstrație. Din teorema 2.1 există șirul de extinderi

$$F = F_0 \subset F_1 \subset \ldots \subset F_r,$$

unde $F = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \ldots, \bar{\alpha}_n)$, $\alpha \in F_r$ și $[F_i : F_{i-1}] \leqslant 2$, $1 \leqslant i \leqslant r$. Rezultă că $[F_r : F] = 2^a$ cu $a \geqslant 0$. Cum $F(\alpha) \subseteq F_r$ și $[F_r : F] = [F(\alpha) : F] \cdot [F_r : F(\alpha)]$, obținem $[F(\alpha) : F] = 2^b$ cu $b \geqslant 0$. Dar $[F(\alpha) : F] = \text{grad } P$, unde P este polinomul minimal al lui α peste corpul $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \ldots, \bar{\alpha}_n)$. Deci grad $P = 2^b$. Dacă facem $n = 2$, atunci $C(\alpha_1, \alpha_2) = C(0, 1)$ și $F = \mathbb{Q}(\alpha_1, \alpha_2, \bar{\alpha}_1, \bar{\alpha}_2) = \mathbb{Q}$.

$C(0, 1)$ se numește *mulțimea numerelor complexe constructibile cu rigla și compasul.* Din teorema 2.1 rezultă că orice număr complex $\alpha \in C(0, 1)$ se exprimă prin radicali.

Aplicații. 1. *Trisecțiunea unghiului.* Vom arăta că nu orice unghi se poate împărți în trei părți egale cu rigla și compasul. De exemplu, fie unghiul de 60°. Unghiul de 60° este determinat de punctele P_1, P_2, P_3 (vezi fig. 18). Numărul complex care are ca afix punctul P_3 este $\alpha_3 = \cos 60° + i \sin 60° = \frac{1}{2} + i\frac{\sqrt{3}}{2}$.

În acest caz $F = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3) = \mathbb{Q}(i\sqrt{3})$. Punctul P este afixul lui $\alpha = \cos 20° + i \sin 20°$. Din identitatea $\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$, făcînd $\varphi = 20°$, obținem

$$\frac{1}{2} = 4\cos^3 20° - 3\cos 20°.$$

Deci cos 20° este rădăcina polinomului ireductibil

$$4X^3 - 3X - \frac{1}{2} \in \mathbb{Q}[X].$$

Întrucît gradul acestui polinom este egal cu trei, gradul polinomului minimal al lui cos 20° peste $\mathbb{Q}(i\sqrt{3})$ este egal cu trei. Din corolarul 2.2 rezultă că cos 20° nu aparține mulțimii $C(0, 1, i\sqrt{3})$ și deci unghiul de 60° nu poate fi împărțit în trei părți egale cu rigla și compasul.

2. *Dublarea cubului.* Vom arăta că fiind dat un cub, nu se poate construi cu rigla și compasul un alt cub care să aibă volumul dublu. Într-adevăr, luăm P_1P_2 egal cu muchia cubului dat. În planul ω, P_1 este originea iar P_2 este de

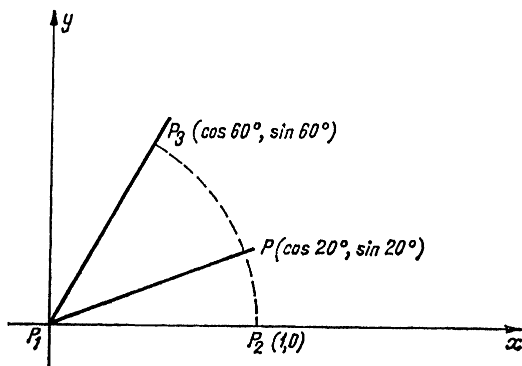


Fig. 18

coordonate (1, 0), adică P_1P_2 este unitatea de măsură. Deci $F = \mathbb{Q}(0, 1) = \mathbb{Q}$. Muchia cubului căutat este $\sqrt[3]{2}$. Deoarece $\sqrt[3]{2}$ are polinomul minimal $X^3 - 2$ peste corpul $\mathbb{Q}$, din corolarul 2.2 rezultă că $\sqrt[3]{2} \notin C(0, 1)$.

3. *Cvadratura cercului.* Vom arăta că fiind dat un cerc, nu se poate construi cu rigla și compasul un pătrat cu aria egală cu aria a cercului dat. Într-adevăr, punctele date din planul ω sînt următoarele: P_1 — centrul cercului și P_2 — un punct de pe cerc. În planul ω se fixează un sistem de axe astfel încît P_1 să fie originea iar P_2 să fie de coordonate (1, 0). Latura pătratului a cărui arie este egală cu a cercului dat este $\sqrt{\pi}$. Numărul π este transcendent peste $\mathbb{Q}$ și deci $\sqrt{\pi}$ este transcendent. Atunci, este evident, că $\sqrt{\pi} \notin C(0, 1)$, ceea ce încheie verificarea afirmației noastre.

4. *Problema celor trei bisectoare.* Vom arăta că nu întotdeauna se poate construi cu rigla și compasul un triunghi, cînd sînt date cele trei bisectoare ale sale. Fie i_a, i_b, i_c, bisectoarele triunghiului ABC iar p semiperimetrul său. Sînt cunoscute formulele:

$$i_a = \frac{2p \sin \frac{B}{2} \sin \frac{C}{2}}{\cos \frac{A}{2} \cos \frac{B-C}{2}},$$

$$i_b = \frac{2p \sin \frac{C}{2} \sin \frac{A}{2}}{\cos \frac{B}{2} \cos \frac{C-A}{2}}, \quad i_c = \frac{2p \sin \frac{A}{2} \sin \frac{B}{2}}{\cos \frac{C}{2} \cos \frac{A-B}{2}}.$$

Presupunem că $i_b = i_c$. Deci $B = C$. Atuni $A + 2B = \pi$ și deci $\cos \frac{A}{2} = \sin B$ și $\sin \frac{A}{2} = \cos B$ și $\cos \frac{C-A}{2} = \sin \frac{3B}{2}$. Rezultă

$$k = \frac{i_a}{i_b} = \frac{\sin \frac{3B}{2}}{2 \cos B}.$$

Notăm $\xi = \sin \frac{B}{2}$. Dacă scriem pe $\sin \frac{3B}{2}$ și $\cos B$ în funcție de ξ, obținem egalitatea

$$4\xi^3 - 4k\xi^2 - 3\xi + 2k = 0.$$

Luăm $k = 3$; atunci ξ este rădăcina polinomului

$$f = 4X^3 - 12X^2 - 3X + 6,$$

care este ireductibil în $Q[X]$. Rezultă că $\xi \notin C(0, 1)$ (conform corolarului 2.2). Deci, nu se poate construi cu rigla și compasul un triunghi isoscel cînd se cunosc cele două bisectoare neegale i_a și i_b, unde $i_a = 3i_b$.

§ 3. Clase conjugate. Formula claselor

Fie G un grup arbitrar. Vom nota

$$C(G) = \{a \in G \mid ax = xa, \text{ oricare ar fi } x \in G\}.$$

Dacă a, $b \in C(G)$, atunci $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$, oricare ar fi $x \in G$. Deci $ab \in C(G)$. Dacă $a \in C(G)$ și $x \in G$, atunci $ax = xa$, de unde rezultă că $x = a^{-1}xa$ și deci $xa^{-1} = a^{-1}x$, adică $a^{-1} \in C(G)$. Deci $C(G)$ este un subgrup al lui G. Acum, dacă $a \in G(C)$ și $x \in G$, atunci $xax^{-1} = axx^{-1} = a$, adică $xax^{-1} \in C(G)$, ceea ce înseamnă că $C(G)$ este un subgrup normal al lui G iar $C(G)$ se numește *centrul grupului* G. Dacă x, $y \in G$, acestea se numesc *conjugate* dacă există $a \in G$ astfel încît $y = axa^{-1}$. Cînd x și y sînt conjugate, notăm $x \overset{c}{\sim} y$. Se

verifică ușor că relația $\overset{c}{\sim}$ este o relație de echivalență pe mulțimea G.

Fie $[x]$ clasa de echivalență a elementului x relativ la această relație de echivalență. Avem

$$[x] = \{y \in G \mid y \overset{c}{\sim} x\} = \{axa^{-1} \mid a \in G\}.$$

Dacă $x \in G$, notăm $C(x) = \{y \in G \mid xy = xy\}$. Se verifică ușor că $C(x)$ este un subgrup al lui G. Subgrupul $C(x)$ se numește *centralizatorul elementului* x.

Lema 3.1. *Fie* $x \in G$. *Atunci* $x \in C(G)$ *dacă și numai dacă* $[x] = \{x\}$ *dacă și numai dacă* $C(x) = G$.

Demonstrația este evidentă.

Propoziția 3.2. *Fie* G *un grup finit și* $x \in G$; *atunci,*

$$\text{card}\,[x] = [G : C(x)].$$

Demonstrație. Definim $\varphi : [x] \to G/R^s$, unde G/R^s este mulțimea claselor de echivalență la stînga modulo subgrupul $C(x)$, în felul următor: dacă $z = axa^{-1} \in [x]$, atunci $\varphi(z) = aC(x)$. Dacă $z = axa^{-1} = bxb^{-1}$, atunci $b^{-1}ax = xb^{-1}a$ și deci $b^{-1}a \in C(x)$, de unde $a\,C(x) = bC(x)$. Rezultă că funcția φ este bine definită. Se vede ușor că φ este surjectivă. Să dovedim că este și injectivă. Fie $\varphi(z) = \varphi(z')$, unde $z = axa^{-1}$ și $z' = a'xa^{-1}$. Atunci $aC(x) = a'C(x)$, de unde rezultă că $a^{-1}a' \in C(x)$ și deci $a^{-1}a'x = xa^{-1}a'$, relație ce implică $axa^{-1} = a'xa'^{-1}$. Deci φ este și injectivă și bijectivă. Să notăm cu R o mulțime de reprezentanți ai claselor conjugate din grupul G.

Teorema 3.3 (*formula claselor*). *Fie* G *un grup finit. Atunci are loc egalitatea*

$$\text{ord}\, G = \text{ord}\, C(G) + \sum_{\substack{x \in R \\ x \notin C(G)}} [G : G(x)].$$

Demonstrație. Din proprietățile claselor de echivalență avem egalitatea

$$G = \bigcup_{x \in R} [x] \text{ (reuniune disjunctă de mulțimi).}$$

Putem scrie

$$G = \bigcup_{\substack{x \in R \\ x \in C(G)}} [x] \cup \bigcup_{\substack{x \in R \\ x \notin C(G)}} [x].$$

Ținînd seama de lema 3.1, obținem $G = C(G) \cup \bigcup_{\substack{x \in R \\ x \notin C(G)}} [x]$.

Trecînd la cardinale și ținînd seama de propoziția 3.2, obținem

$$\text{card}\, G = \text{card}\, C(G) + \sum_{\substack{x \in R \\ x \notin C(G)}} \text{card}\, [x]$$

sau

$$\text{ord}\, G = \text{ord}\, C(G) + \sum_{\substack{x \in R \\ x \notin C(G)}} [G : C(x)].$$

Fie p un număr prim. Un grup finit G se numește *p-grup* dacă $\text{ord}\, G = p^n (n \geqslant 1)$.

Corolarul 3.4. *Dacă G este un p-grup, atunci*

$$C(G) \neq \{e\}.$$

Demonstrație. Scriem formula claselor

$$\text{ord}\, G = \text{ord}\, C(G) + \sum_{\substack{x \in R \\ x \notin C(G)}} [G : C(x)].$$

Dacă $x \in R$ și $x \notin C(G)$, atunci $C(x) \neq G$ și deci $[G : C(x)] > 1$. Din teorema lui Lagrange și din faptul că G este p-grup obținem că $p \mid [G : C(x)]$. Atunci $p \mid \sum_{\substack{x \in R \\ x \notin C(G)}} [G : C(x)]$. Cum $p \mid \text{ord}\, G$, rezultă $p \mid \text{ord}\, C(G)$ și deci $C(G)$ are cel puțin p elemente. Deci $C(G) \neq \{e\}$.

Corolarul 3.5. *Dacă G este p-grup, atunci G este rezolubil.*

Demonstrație. Fie $\text{ord}\, G = p^n$ $(n \geqslant 1)$. Dacă $n = 1$, atunci $\text{ord}\, G = p$ și G este ciclic, deci abelian și rezolubil. Presupunem afirmația adevărată pentru $k \leqslant n - 1$ și verificăm pentru n. Din corolarul 3.4 avem că $p \mid \text{ord}\, C(G)$. Din teorema lui Lagrange obținem că $\text{ord}\, G/C(G) = p^k$ cu $k \leqslant n - 1$. Din ipoteza de inducție obținem că $G/C(G)$ este rezolubil. Dar $C(G)$ fiind abelian, deci rezolubil, din teorema 1.3, cap. VII, rezultă că G este rezolubil.

§ 4. Al doilea criteriu de constructibilitate cu rigla și compasul

Fie K un corp (de numere complexe). O extindere E a lui K se numește *pitagoreică* dacă există un șir de extinderi

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_r = E$$

astfel încît $[K_i : K_{i-1}] \leqslant 2$, pentru orice $1 \leqslant i \leqslant r$. Se observă imediat că pentru $1 \leqslant i \leqslant r$, K_i este o extindere radicală simplă a lui K_{i-1} și deci orice extindere pitagoreică a corpului K este o extindere radicală.

Teorema 4.1. *Dacă E este o extindere pitagoreică a corpului K, atunci există o extindere normală și pitagoreică F a lui K astfel încît $E \subseteq F$.*

Demonstrația se face la fel ca cea a teoremei 4.1, cap. VII.

Teorema 4.2. *Fie E o extindere normală a corpului K. Atunci E este o extindere pitagoreică a corpului K dacă și numai dacă $[E : K]$ este o putere a lui* 2.

Demonstrație. Presupunem mai întîi că E este o extindere pitagoreică a lui K. Există un șir de extinderi

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_r = E,$$

unde $[K_i : K_{i-1}] \leqslant 2$, $1 \leqslant i \leqslant r$. Rezultă că $[E : K] = 2^s$ $(s \geqslant 0)$. Reciproc, presupunem că $[E : K] = 2^n$. Vom nota cu G grupul Galois $G(E/K)$ al cărui ordin este 2^n. Să notăm cu Z_1 centrul lui G. Din corolarul 3.4 avem $Z_1 \neq \{e\}$. Cum G/Z_1 este un 2-grup, atunci centrul său, care este de forma Z_2/Z_1, are cel puțin două elemente. În acest fel obținem șirul crescător de subgrupuri ale lui G

(1) $$Z_1 \subset Z_2 \subset \ldots \subset Z_{i-1} \subset Z_i \subset \ldots,$$

unde Z_i/Z_{i-1} este centrul grupului G/Z_{i-1}. Cum G este finit și pentru orice $i \geqslant 1$ avem că Z_i/Z_{i-1} are cel puțin două elemente, există un $r \geqslant 1$ astfel încît $G = Z_r$. Deoarece Z_i/Z_{i-1} este comu-

tativ și are ordinul o putere a lui 2, făcînd eventual o rafinare a șirului (1), obținem un șir normal de subgrupuri ale lui G

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_s = G,$$

astfel încît $[H_i : H_{i-1}] = 2$, $1 \leqslant i \leqslant s$. Dacă notăm $K_i = E^H_{s-i}$, unde $0 \leqslant i \leqslant s$, obținem șirul de extinderi

$$K = K_0 \subset K_1 \subset \ldots \subset K_s = E.$$

Din teorema fundamentală a lui Galois obținem $[K_i : K_{i-1}] = 2$, pentru orice $1 \leqslant i \leqslant s$. Rezultă că E este o extindere pitagoreică a corpului K.

Corolarul 4.3 (*criteriul al doilea de constructibilitate cu rigla și compasul*). *Fie $\alpha_1, \alpha_2, \ldots, \alpha_n$ numere complexe ($n \geqslant 1$). Numărul complex α este constructibil cu rigla și compasul din numerele $\alpha_1, \alpha_2, \ldots, \alpha_n$ dacă există o extindere normală E a corpului $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \ldots, \bar{\alpha}_n)$ de grad egal cu o putere a lui 2 astfel încît $\alpha \in E$.*

Demonstrație. Dacă α este constructibil cu rigla și compasul din numerele $\alpha_1, \alpha_2, \ldots, \alpha_n$, din teorema 2.1 rezultă că există o extindere pitagoreică E' a lui $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \ldots, \bar{\alpha}_n)$ cu $\alpha \in E'$. În continuare aplicăm teorema 4.1 și 4.2. Reciproca se obține din teorema 4.1 și teorema 2.1.

§ 5. Construcția poligoanelor regulate cu rigla și compasul

A construi un poligon cu n laturi revine la a împărți un cerc dat în n părți egale. Punctele care se dau în planul ω sînt P_1 (centrul cercului) și P_2 (un punct de pe cerc). În planul ω se ia un sistem ortogonal de axe cu originea în P_1 astfel încît P_2 să fie de coordonate (1, 0). În acest caz, mulțimii $C(P_1, P_2)$ i se asociază corpul de numere complexe $C(0, 1)$. Ca să împărțim cercul în n părți egale cu rigla și compasul trebuie să arătăm că numerele $\cos \frac{2\pi}{n}$ și $\sin \frac{2\pi}{n}$ aparțin mulțimii $C(0, 1)$

sau, echivalent, că $\xi = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n} \in C(0, 1)$. Numărul ξ este rădăcină primitivă a ecuației

$$x^n - 1 = 0.$$

Deci $\mathbb{Q}(\xi)$ este o extindere normală a corpului $\mathbb{Q}$ (fiind corpul de descompunere al polinomului $X^n - 1$). Aplicînd cel de-al doilea criteriu de constructibilitate cu rigla și compasul, ξ este constructibil cu rigla și compasul dacă și numai dacă există o extindere normală E a lui $\mathbb{Q}$ astfel încît $\xi \in E$ și $[E : Q] = 2^s$. Cum $\mathbb{Q}(\xi) \subseteq E$, atunci $[\mathbb{Q}(\xi) : \mathbb{Q}] = 2^r$. Deci ξ este constructibil cu rigla și compasul dacă și numai dacă $[\mathbb{Q}(\xi) : \mathbb{Q}]$ este o putere a lui 2.

Teorema 5.1. $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$, *unde* $\varphi(n)$ *este indicatorul lui Euler al numărului natural* n.

Demonstrație. Fie G grupul Galois al polinomului $X^n - 1$. Deci $G = G(\mathbb{Q}(\xi)/\mathbb{Q})$. Fie $\mathbb{Z}_n^*$ grupul unităților inelului $\mathbb{Z}_n$, deci $\mathbb{Z}_n^* = \{\hat{a} \mid (a, n) = 1\}$. Ordinul grupului $\mathbb{Z}_n^*$ este $\varphi(n)$. Definim aplicația

$$\alpha : G \to \mathbb{Z}_n^*$$

în felul următor : dacă $\sigma \in G$, atunci $\sigma(\xi) = \xi^a$. Punem $\alpha(\sigma) = \hat{a}$. Această aplicație este un omomorfism de grupuri (a se vedea teorema 3.1, cap. VII). Dacă $\alpha(\sigma) = \hat{a} = \hat{1}$, atunci $n \mid (a - 1)$ și deci există un număr întreg k astfel încît $a - 1 = kn$, adică $a = kn + 1$. Cum $\sigma(\xi) = \xi^a$, atunci $\sigma(\xi) = \xi^{kn+1} = (\xi^n)^k \cdot \xi = \xi$. Din $\mathbb{Q}(\xi) = \mathbb{Q}[\xi]$ rezultă că pentru orice $x \in \mathbb{Q}(\xi)$ avem $\sigma(x) = x$, adică $\sigma = 1_{\mathbb{Q}(\xi)}$. Deci α este o funcție injectivă. Rezultă că ord $G \leqslant$ ord $\mathbb{Z}_n^* = \varphi(n)$. Deci inegalitatea $[\mathbb{Q}(\xi) : \mathbb{Q}] \leqslant \varphi(n)$ este demonstrată.

Fie $f_n(X) \in \mathbb{Q}[X]$ polinomul minimal al lui ξ. Cum $[\mathbb{Q}(\xi) : \mathbb{Q}] =$ grad (f_n), vom demonstra că grad $f_n \geqslant \varphi(n)$. Pentru aceasta, vom arăta că pentru orice număr natural k, $1 \leqslant k < n$, $(k, n) = 1$, ξ^k este o rădăcină a lui $f_n(X)$. Deoarece $f_n \mid (X^n - 1)$, putem să scriem $X^n - 1 = f_n \cdot h$ cu $h \in \mathbb{Q}[X]$. Dar $X^n - 1$ are coeficienți în $\mathbb{Z}$, deci $f_n, h \in \mathbb{Z}[X]$. Pentru a arăta că ξ^k este rădăcină a lui f_n cînd $(k, n) = 1$, este suficient să arătăm aceasta cînd k este un număr prim. Prin absurd, presupunem că există un număr prim p astfel încît $1 < p < n$, $(p, n) = 1$ și ξ^p nu este rădăcină a lui f_n. Cum $f_n(\xi^p) \neq 0$, atunci $h(\xi^p) = 0$. Deci

ξ este rădăcină a polinomului $h(X^p)$. Atunci $f_n | h(X^p)$, adică există $g \in \mathbb{Z}[X]$ astfel încît $h(X^p) = f_n g$. Utilizînd teorema lui Fermat, avem $h(X)^p \equiv h(X)$ (mod p) în sensul că p divide coeficienții polinomului $h(X)^p - h(X)$. Dacă $u(X) = a_0 + a_1 X + \dots$ $\dots + a_r X^r \in \mathbb{Z}[X]$, notăm cu $\bar{u}(X)$ polinomul din $\mathbb{Z}_p[X]$ definit astfel:

$$\bar{u}(X) = \hat{a}_0 + \hat{a}_1 X + \dots + \hat{a}_r X^r.$$

Cu această notație avem egalitățile

$$X^n - \hat{1} = \bar{f}_n \bar{h}, \quad \bar{h}(X^p) = \bar{f}_n \bar{g}, \quad \bar{h}(X^p) = \bar{h}(X)^p.$$

Fie K o extindere a corpului $\mathbb{Z}_p$ în care $\bar{f}_n(X)$ are o rădăcină α. Atunci α este o rădăcină a lui $\bar{h}(X^p)$ și deci a lui $\bar{h}(X)^p$. Din $\bar{h}(\alpha)^p = 0$ rezultă $\bar{h}(\alpha) = 0$, adică α este rădăcină a lui $\bar{f}_n$ și $\bar{h}$. Deci α este rădăcină dublă a lui $X^n - \hat{1}$. Rezultă că α anulează derivata polinomului $X^n - \hat{1}$ care este nX^{n-1}. Deci $n\,\alpha^{n-1} = 0$. Din $(p, n) = 1$, rezultă că $\alpha^{n-1} = 0$, de unde $\alpha = 0$. Deoarece α este rădăcină a lui $X^n - \hat{1}$, rezultă că $\hat{1} = 0$, ceea ce reprezintă o contradicție. Deci presupunerea că ξ^p nu este rădăcină a lui f_n ne-a dus la o contradicție.

Observații. Din demonstrația teoremei 5.1 rezultă:

1. Grupul Galois $G = G(\mathbb{Q}(\xi)/\mathbb{Q}) \simeq \mathbb{Z}_n^*$.
2. Polinomul minimal al elementului ξ peste $\mathbb{Q}$ este

$$f_n(X) = \prod_{(k,n)=1} (X - \xi^k).$$

Dacă $n = 2^a p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$, unde $a \geq 0$, $p_1, p_2, \dots, p_k$ sînt numere prime distincte și diferite de 2, atunci

$$\varphi(n) = 2^{a-1} p_1^{n_1-1}(p_1 - 1) \dots p_k^{n_k-1}(p_k - 1)$$

este o putere a lui 2 dacă și numai dacă $n_1 = n_2 = \dots = n_k = 1$ și $p_1 - 1, \dots, p_k - 1$ sînt puteri ale lui 2. Scriem $p_i - 1 = 2^{m_i} (1 \leq i \leq k)$, $p_i = 2^{m_i} + 1$. Ca p_i să fie prim trebuie ca m_i să fie o putere a lui 2. Într-adevăr, putem scrie $m_i = 2^{t_i} \cdot u$, unde u este un număr impar. Atunci $p_i = 2^{2^{t_i} u} + 1 = (2^{2^{t_i}})^u + 1$. Deoarece u este impar, $2^{2^{t_i}} + 1$ divide pe p. Deci ca p_i să fie prim trebuie ca $u = 1$ și $m_i = 2^{t_i}$. Atunci $p_i = 2^{2^{t_i}} + 1$.

Numerele prime de forma $p = 2^{2^n} + 1$ se numesc *numere prime ale lui Fermat.*

Este cunoscut că pentru $n = 1, 2, 3, 4$ numerele care se obțin sînt numere prime. Acestea sînt $p = 3, 5, 17, 257, 65537$. Pentru $n = 5$, Euler a arătat că $2^{32} + 1 = 641 \times 6700417$, deci nu este număr prim.

Teorema 5.2. *Un poligon regulat cu n laturi se poate construi cu rigla și compasul dacă și numai dacă n este de forma* $2^{\alpha} p_1 p_2 \ldots p_k$, *unde* $p_1, p_2, \ldots, p_k$ *sînt numere prime ale lui Fermat distincte între ele.*

Din teorema 5.2 rezultă, în particular, că se pot construi, de exemplu, poligoanele regulate cu 4, 8, 16, 32, ... laturi. De asemenea se pot construi poligoanele regulate cu 5 și 17 laturi.

Scurt istoric. Problema construcției figurilor geometrice cu rigla și compasul a stat în atenția matematicienilor încă din antichitate, în special, își are originea în matematica greacă. Cele mai notabile probleme care au apărut atunci sînt: 1) trisecțiunea unghiului; 2) dublarea cubului; 3) cvadratura cercului și 4) construcția poligonului regulat cu șapte laturi (heptagonul regulat). Așa cum am văzut, cele patru probleme au un răspuns negativ. Dar acest lucru a fost demonstrat mult mai tîrziu. De exemplu, problema cvadraturii cercului a fost posibilă de a primi un răspuns negativ numai după ce F. Lindemann în 1882 a arătat că numărul π este transcendent.

Problema generală a determinării numerelor naturale n pentru care se pot construi cu rigla și compasul poligoanele regulate cu n laturi a fost complet rezolvată de Gauss în celebra sa lucrare „Disquisitiones Arithmeticae" (1801).

BIBLIOGRAFIE

1. Artin, E. *Galoische Theorie*. Leipzig, B. G. Teubner, 1965.
2. Galbură, Gh. *Corpuri de funcții algebrice și varietăți algebrice*. București, Editura Academiei, R.P.R., 1961.
3. Ion, D. I., Radu, N. *Algebră*. București, Editura didactică și pedagogică, 1975.
4. Ionescu, V. *Algebră*. București, Editura didactică și pedagogică, 1960.
5. Jacobson, N. *Basic Algebra I*. San Francisco, Freeman, 1974.
6. Kuroș, A. G. *Curs de algebră superioară* (trad. din l. rusă). București, Editura tehnică, 1955.
7. Lang, S. *Algebra*. Addison-Wesley, Publ. Co., Reading Mass, 1965.
8. Mac Lane S., Birkhoff, G. *Algebra*. New York, London, Collier-Macmillan, 1967.
9. Năstăsescu, C. *Inele, module, categorii*. București, Editura Academiei, 1976.
10. Niță, C., Spircu, T. *Probleme de structuri algebrice*. București, Editura tehnică, 1974.
11. Postnikov, M. M. *Teoria Galua*. Moscova, 1963.
12. Sâmboan, G. *Teoria lui Galois*. București, Editura tehnică, 1968.